DeviceLock®

Manuel d'utilisation

Version du logiciel 7.1

© 1996-2012 DeviceLock, Inc. Tous droits réservés.

Les informations contenues dans ce document sont sujettes à modifications sans préavis. Aucune partie de ce document ne peut être reproduite ou transmise, sous quelque forme ou de quelque façon que ce soit, dans un but autre que l'utilisation personnelle de l'acheteur, sans l'autorisation écrite préalable de DeviceLock, Inc.

Marques commerciales

DeviceLock et le logo DeviceLock sont des marques commerciales déposées de DeviceLock, Inc. Tous les autres noms de produits, marques de service et marques commerciales mentionnés dans les présentes sont des marques commerciales de leurs propriétaires respectifs.

DeviceLock - Manuel d'utilisation
Version du logiciel: 7.1
Mise à jour: mars 5, 2012

Table des matières

A PROPOS DE CE MANUEL 6
CONVENTIONS 6
PRESENTATION 7
INFORMATIONS GENERALES 7
CONTROLE D'ACCES GERE AUX PERIPHERIQUES ET AUX PROTOCOLES 11
COMPRENDRE DEVICELOCK CONTENT SECURITY SERVER 16
MODE DE FONCTIONNEMENT DE SEARCH SERVER 16
EXTENSION DES FONCTIONNALITES DE DEVICELOCK AVEC CONTENTLOCK ET NETWORKLOCK 18
LICENCES 22
MESURES DE SECURITE DE BASE RECOMMANDEES 23
INSTALLATION 25
PREREQUIS 25
DEPLOIEMENT DE DEVICELOCK SERVICE 25
INSTALLATION INTERACTIVE 25
INSTALLATION AUTOMATIQUE 32
INSTALLATION VIA MICROSOFT SYSTEMS MANAGEMENT SERVER 34
INSTALLATION A DISTANCE VIA DEVICELOCK MANAGEMENT CONSOLE 34
INSTALLATION A DISTANCE VIA DEVICELOCK ENTERPRISE MANAGER 35
INSTALLATION VIA GROUP POLICY 37
INSTALLATION DES CONSOLES DE GESTION 45
INSTALLATION DE DEVICELOCK ENTERPRISE SERVER 53
PLANIFICATION DE L'INFRASTRUCTURE 54
INSTALLATION INTERACTIVE 54
INSTALLATION DE DEVICELOCK CONTENT SECURITY SERVER 72
DEVICELOCK CERTIFICATES 81
PRESENTATION 81
CREATION DE DEVICELOCK CERTIFICATES 81
INSTALLATION ET SUPPRESSION DE DEVICELOCK CERTIFICATES 83
DEVICELOCK SIGNING TOOL 88
PRESENTATION 88
DEVICE CODE (CODE DE PERIPHERIQUE) 88
SERVICE SETTINGS (PARAMETRES DE SERVICE) 90
DEVICELOCK MANAGEMENT CONSOLE 94
PRESENTATION 94
INTERFACE 96
CONNEXION AUX ORDINATEURS 97

ERREURS DE CONNEXION POSSIBLES 100
ADMINISTRATION DE DEVICELOCK SERVICE 101
SERVICE OPTIONS (OPTIONS DE SERVICE) 103
DEVICES (PERIPHERIQUES) 128
PERMISSIONS (AUTORISATIONS) (REGULAR PROFILE) 129
AUDITING & SHADOWING (AUDIT ET REPLICATION) (REGULAR PROFILE) 138
USB DEVICES WHITE LIST (LISTE BLANCHE DE PERIPHERIQUES USB) (REGULAR PROFILE) 149
MEDIA WHITE LIST (LISTE BLANCHE DE MEDIAS) (REGULAR PROFILE) 154
SECURITY SETTINGS (PARAMETRES DE SECURITE) (REGULAR PROFILE) 158
AUDIT LOG VIEWER (SERVICE) 161
SHADOW LOG VIEWER (SERVICE) 166
ADMINISTRATION DE DEVICELOCK ENTERPRISE SERVER 173
SERVER OPTIONS (OPTIONS DE SERVEUR) 174
AUDIT LOG VIEWER (SERVER) 175
SHADOW LOG VIEWER (SERVER) 179
SERVER LOG VIEWER 183
SURVEILLANCE 186
GESTION ET UTILISATION DE DEVICELOCK CONTENT SECURITY SERVER 200
PARCOURIR DEVICELOCK CONTENT SECURITY SERVER 200
CONFIGURATION DES PARAMETRES GENERAUX DE DEVICELOCK CONTENT SECURITY SERVER 202
CONFIGURATION DES PARAMETRES DE RECHERCHE SYSTEMATIQUE DE TEXTE POUR SEARCH SERVER 207
UTILISATION DE SEARCH SERVER 215
DEVICELOCK GROUP POLICY MANAGER 226
PRESENTATION 226
APPLIQUER UNE POLITIQUE DE GROUPE 227
REGLES DE TRANSMISSION DE GPO STANDARD 227
DEMARRAGE DE DEVICELOCK GROUP POLICY MANAGER 228
UTILISATION DE DEVICELOCK GROUP POLICY MANAGER 232
UTILISATION DE RSOP (RESULTANT SET OF POLICY) 235
DEVICELOCK SERVICE SETTINGS EDITOR 238
PRESENTATION 238
DEVICELOCK ENTERPRISE MANAGER 240
PRESENTATION 240
INTERFACE 241
BOITE DE DIALOGUE SCAN NETWORK 242
SELECTION DES ORDINATEURS 243
SELECTION DES PLUG-INS 249
DEMARRER UN SCAN 249
PLUG-INS 250
AUDIT LOG VIEWER (VISIONNEUR DE JOURNAL D'AUDIT) 251
INSTALL SERVICE (SERVICE D'INSTALLATION) 251

REPORT PERMISSIONS/AUDITING 252
REPORT PNP DEVICES (ETAT DES PERIPHERIQUES PNP) 253
SET SERVICE SETTINGS (DEFINITION DES PARAMETRES DE SERVICE) 255
SHADOW LOG VIEWER (VISIONNEUR DE JOURNAL DE REPLICATION) 256
UNINSTALL SERVICE (SERVICE DE DESINSTALLATION)..... 256
OUVERTURE / SAUVEGARDE / EXPORT 256
COMPARAISON DE DONNEES 258
FILTRAGE DE DONNEES..... 262
REGLES CONTEXTUELLES POUR LES PERIPHERIQUES (REGULAR PROFILE) 265
REGLES CONTEXTUELLES POUR OPERATIONS DE CONTROLE D'ACCES..... 266
REGLES CONTEXTUELLES POUR COPIES DE REPLICATION..... 270
CONFIGURATION DE PARAMETRES DE DETECTION DE CONTENU 271
GROUPES FILE TYPE DETECTION CONTENT..... 272
GROUPES DE CONTENUS KEYWORDS 276
GROUPES DE CONTENUS PATTERN..... 281
GROUPES DE CONTENUS DOCUMENT PROPERTIES 285
GROUPES A CONTENUS COMPLEXES..... 290
CONSULTER LES GROUPES DE CONTENUS INTEGRES 293
DUPLIQUER LES GROUPES DE CONTENUS INTEGRES 293
MODIFICATION ET SUPPRESSION D'UN GROUPE DE CONTENUS PERSONNALISE..... 294
TEST DES GROUPES DE CONTENUS..... 295
GESTION DES REGLES CONTEXTUELLES..... 296
DEFINITION DE REGLES CONTEXTUELLES 296
MODIFICATION DE REGLES CONTEXTUELLES..... 300
COPIE DE REGLES CONTEXTUELLES 301
EXPORTATION ET IMPORTATION DE REGLES CONTEXTUELLES 302
REVOCATION DE REGLES CONTEXTUELLES..... 304
SUPPRESSION DE REGLES CONTEXTUELLES 305
REGLES CONTEXTUELLES POUR LES PROTOCOLES (REGULAR PROFILE) ...307
REGLES CONTEXTUELLES POUR OPERATIONS DE CONTROLE D'ACCES..... 307
REGLES CONTEXTUELLES POUR OPERATIONS DE COPIE DE REPLICATION..... 310
CONFIGURATION DE PARAMETRES DE DETECTION DE CONTENU 311
GROUPES FILE TYPE DETECTION CONTENT..... 312
GROUPES DE CONTENUS KEYWORDS 316
GROUPES DE CONTENUS PATTERN..... 321
GROUPES DE CONTENUS DOCUMENT PROPERTIES 325
GROUPES A CONTENUS COMPLEXES..... 329
CONSULTER LES GROUPES DE CONTENUS INTEGRES 332
DUPLIQUER LES GROUPES DE CONTENUS INTEGRES 332
MODIFICATION ET SUPPRESSION D'UN GROUPE DE CONTENUS PERSONNALISE..... 333
TEST DES GROUPES DE CONTENUS..... 334
GESTION DES REGLES CONTEXTUELLES..... 335
DEFINITION DE REGLES CONTEXTUELLES 335

MODIFICATION DE REGLES CONTEXTUELLES 339
COPIE DE REGLES CONTEXTUELLES 340
EXPORTATION ET IMPORTATION DE REGLES CONTEXTUELLES 341
REVOCATION DE REGLES CONTEXTUELLES 343
SUPPRESSION DE REGLES CONTEXTUELLES 344

PROTOCOLES (REGULAR PROFILE) 345

GESTION DES AUTORISATIONS DE PROTOCOLES 346
DEFINITION ET EDITION D'AUTORISATIONS 350
REVOCATION D'AUTORISATIONS 352

GESTION DES REGLES D'AUDIT ET DE REPLICATION DE PROTOCOLES 353
DEFINITION ET EDITION DE REGLES D'AUDIT ET DE REPLICATION 362
REVOCATION DE REGLES D'AUDIT ET DE REPLICATION 365

GESTION DE LA LISTE BLANCHE DE PROTOCOLES 365
DEFINITION DE LA LISTE BLANCHE DE PROTOCOLES 370
ÉDITION DE LISTE BLANCHE DE PROTOCOLES 373
COPIE DES REGLES DE LA LISTE BLANCHE DE PROTOCOLES 374
EXPORTATION ET IMPORTATION DE LISTE BLANCHE DE PROTOCOLES 376
REVOCATION DE LISTE BLANCHE DE PROTOCOLES 378
SUPPRESSION DE REGLES DE LISTE BLANCHE DE PROTOCOLES 378

GESTION DES PARAMETRES DE SECURITE POUR LES PROTOCOLES 379
DEFINITION ET MODIFICATION DE PARAMETRES DE SECURITE 380
REVOCATION DE PARAMETRES DE SECURITE 381

RAPPORTS DEVICELOCK 382

CATEGORIES ET TYPES DE RAPPORTS 382
AUDIT LOG REPORTS 383
SHADOW LOG REPORTS 387

CONFIGURATION D'ENVOI DE RAPPORTS PAR E-MAILS 390

CONFIGURATION DE FORMAT DE RAPPORTS PAR DEFAUT 392

DEFINITION DE PARAMETRES DE RAPPORT 392
BOITE DE DIALOGUE REPORT OPTIONS 392

GESTION DE RAPPORTS 398
EXECUTION DE RAPPORTS 399
MISE A JOUR DE RAPPORTS 400
AFFICHAGE DE RAPPORTS 400
AFFICHAGE DE PARAMETRES DE RAPPORTS 401
EXPORTATION ET ENREGISTREMENT DE RAPPORTS 401
ENVOI DE RAPPORTS PAR E-MAIL 402
SUPPRESSION DE RAPPORTS 403

POLITIQUES DE SECURITE DE DEVICELOCK (OFFLINE PROFILE) 405

CONFIGURATION DE PARAMETRES DE DETECTION DE MODE HORS LIGNE 406

PASSAGE DU MODE EN LIGNE AU MODE HORS LIGNE 408

GESTION DES POLITIQUES DE SECURITE HORS LIGNE
POUR LES PERIPHERIQUES 409
GESTION DES AUTORISATIONS HORS LIGNE 409
GESTION DES REGLES D'AUDIT ET DE REPLICATION HORS LIGNE 414

GESTION DE LA LISTE BLANCHE DE PERIPHERIQUES USB HORS LIGNE 419
GESTION DE LA LISTE BLANCHE DE MEDIAS HORS LIGNE 426
GESTION DES REGLES CONTEXTUELLES HORS LIGNE POUR LES PERIPHERIQUES 433
GESTION DES PARAMETRES DE SECURITE HORS LIGNE 444
GESTION DES POLITIQUES DE SECURITE HORS LIGNE POUR LES PROTOCOLES 449
GESTION DES AUTORISATIONS HORS LIGNE POUR LES PROTOCOLES 449
GESTION DES REGLES D'AUDIT ET DE REPLICATION HORS LIGNE DES PROTOCOLES 454
GESTION DE LA LISTE BLANCHE DE PROTOCOLES HORS LIGNE 459
GESTION DES REGLES CONTEXTUELLES POUR LES PROTOCOLES HORS LIGNE 469
GESTION DES PARAMETRES DE SECURITE DES PROTOCOLES HORS LIGNE 480
TEMPORARY WHITE LIST 484
PRESENTATION 484
TEMPORARY WHITE LIST AUTHORIZATION TOOL 485
ANNEXE 488
EXEMPLES D'AUTORISATIONS ET D'AUDIT DE PERIPHERIQUES 488
EXEMPLES D'AUTORISATIONS 488
EXEMPLES DE REGLES D'AUDIT ET DE REPLICATION 499
EXEMPLES D'AUTORISATIONS DE PROTOCOLES 502
EXEMPLES DE REGLES CONTEXTUELLES 505

A propos de ce manuel

Ce manuel contient des informations détaillées sur le mode d'installation et d'utilisation de DeviceLock. Il est avant tout conçu pour les administrateurs, les responsables sécurité, et les autres informaticiens spécialisés dans les problèmes de sécurité des données au sein de l'entreprise.

Ce manuel présuppose des connaissances de base du système d'exploitation Microsoft Windows et de la gestion de réseau, ainsi que la possibilité de créer un réseau local (LAN).

Conventions

Le tableau suivant contient une liste des conventions utilisées dans ce manuel.

CONVENTION	DESCRIPTION
Texte en gras	Indique des éléments d'interface utilisateur comme les menus et les commandes, ainsi que les titres et options de boîtes de dialogue.
Texte en italiques	Utilisé pour les commentaires.
Texte en bleu	Indique des liens hypertexte.
Remarque	Utilisé pour fournir des informations complémentaires.
Attention	Utilisé pour vous avertir de problèmes éventuels.
Pratiques éprouvées	Utilisé pour fournir des recommandations en matière de pratiques éprouvées.
Signe plus (+)	Utilisé pour indiquer une combinaison de touches à actionner en même temps.

Présentation

Informations générales

En matière de protection et de gestion des réseaux d'entreprise, il est important d'empêcher les échanges de données et de logiciels indésirables. Pendant longtemps, les administrateurs n'ont pas eu d'autre solution que d'obstruer les lecteurs de disquettes pour éviter les problèmes. Facile à installer, DeviceLock permet aux administrateurs réseau d'appliquer des restrictions d'accès planifiées aux ports USB, série ou parallèles, aux lecteurs de disquettes et de CD-ROM et à tous les autres périphériques à média amovibles, aux adaptateurs Wifi et Bluetooth, ainsi qu'aux ports USB, FireWire, Infrarouge etc. Et ce, sans avoir à les retirer ou à les verrouiller physiquement.

NetworkLock, une extension de DeviceLock, permet de contrôler les communications réseau. Les administrateurs peuvent appliquer des restrictions d'accès planifiées aux protocoles FTP, HTTP, SMTP, Telnet, aux messageries instantanées (ICQ, AOL, Windows Live Messenger, Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), aux applications de messagerie Web et de réseaux sociaux (AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, et Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING).

ContentLock, une autre extension de DeviceLock, extrait et filtre les données copiées sur des disques amovibles et des périphériques de stockage plug-and-play, ainsi que les données transmises sur le réseau. Les administrateurs peuvent créer des règles régissant la nature des données susceptibles d'être copiées ou transmises.

DeviceLock permet à l'administrateur de connaître précisément le type de périphérique ou le protocole en activité sur un ordinateur local. DeviceLock emploie le sous-système d'enregistrement d'événements standard et inscrit les rapports dans le registre des événements Windows.

DeviceLock permet la réplication des données transférées, autrement dit la restitution de toute donnée copiée vers une solution de stockage externe, transférée par un port parallèle ou série, ou transmise sur le réseau. Le programme peut sauvegarder une copie complète des fichiers dans la base de données SQL. Il est possible de définir la réplication, comme les rapports d'activité, utilisateur par utilisateur.

De plus, les données de la fonction de réplication de DeviceLock sont compatibles avec la National Software Reference Library (bibliothèque de référence des logiciels) sous le contrôle du National Institute of Standards and Technology (Institut national des standards et de la technologie, NIST) comme avec la Hashkeeper Database, table de hachage conçue et gérée par le National Drug Intelligence Center (Centre

national des renseignements sur les stupéfiants) du Ministère de la justice des Etats-Unis.

On peut vérifier les données enregistrées sous DeviceLock en les comparant aux tables de hachage (listes des signatures numériques de données connues et d'origine vérifiable).

Vous pouvez aussi créer votre propre base de données de signatures numériques (les formats SHA-1, MD5 et CRC32 sont compatibles) ou des fichiers critiques et l'utiliser ensuite à des fins de suivi. Vous pouvez par exemple savoir qui copie des fichiers signés, à quelle heure et sur quel support.

Pour plus d'information sur le mode d'emploi des tables de hachage avec DeviceLock, veuillez contacter notre équipe de support technique.

Vous trouverez plus d'information au sujet des tables de hachage et de leurs échantillons sur le site Web de la National Software Reference Library: http://www.nsrl.nist.gov.

DeviceLock permet aussi les recherches instantanées de texte dans les fichiers masqués et l'examen des journaux stockés dans la base de données centralisée. DeviceLock peut automatiquement reconnaître, indexer, rechercher et afficher les documents dans de nombreux formats, notamment: Adobe Acrobat (PDF), Ami Pro, Archives (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documents, feuilles de calcul et présentations), Quattro Pro, WordPerfect, WordStar et plus encore.

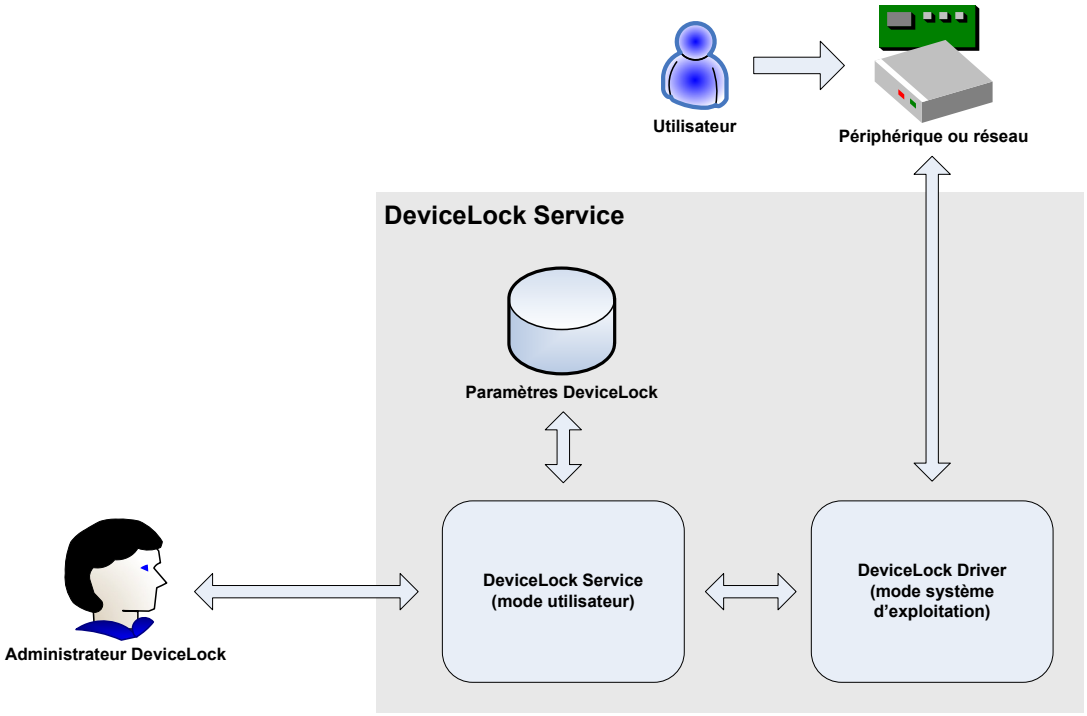
Outre l'administration normale des autorisations (ordinateur par ordinateur), DeviceLock propose aussi un mécanisme plus puissant, qui permet de modifier et de déployer les autorisations et les paramètres via les Politiques de groupe dans un domaine Active Directory.

DeviceLock permet également une meilleure intégration dans Active Directory. Pour les administrateurs système, cette fonctionnalité clé facilite grandement la gestion des autorisations et le déploiement dans le cadre de réseaux conséquents.

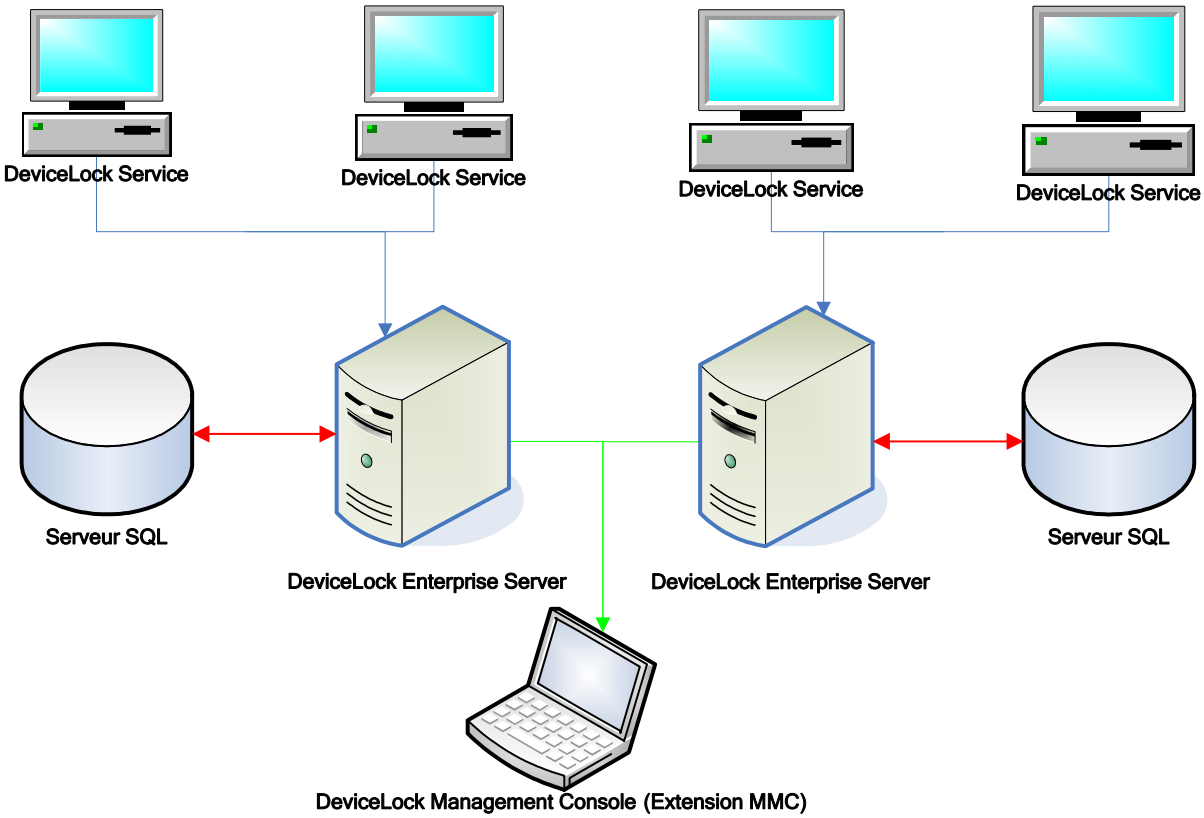
Grâce à l'intégration dans Active Directory, il n'est plus nécessaire d'installer des applications tierces en cas d'administration centralisée, et lors du déploiement. Avec DeviceLock, nul besoin d'avoir sa propre version à base de serveurs pour contrôler la totalité du réseau; les fonctions standards fournies par Active Directory suffisent.

DeviceLock est constitué de trois parties: le client (DeviceLock Service), le serveur (DeviceLock Enterprise Server et DeviceLock Content Security Server) et la console de gestion (DeviceLock Management Console, DeviceLock Group Policy Manager ou DeviceLock Enterprise Manager).

1. DeviceLock Service est le cœur de DeviceLock. Il s'installe sur chaque système client, s'exécute automatiquement et fournit une protection d'accès et au réseau sur la machine client tout en demeurant invisible aux utilisateurs locaux.

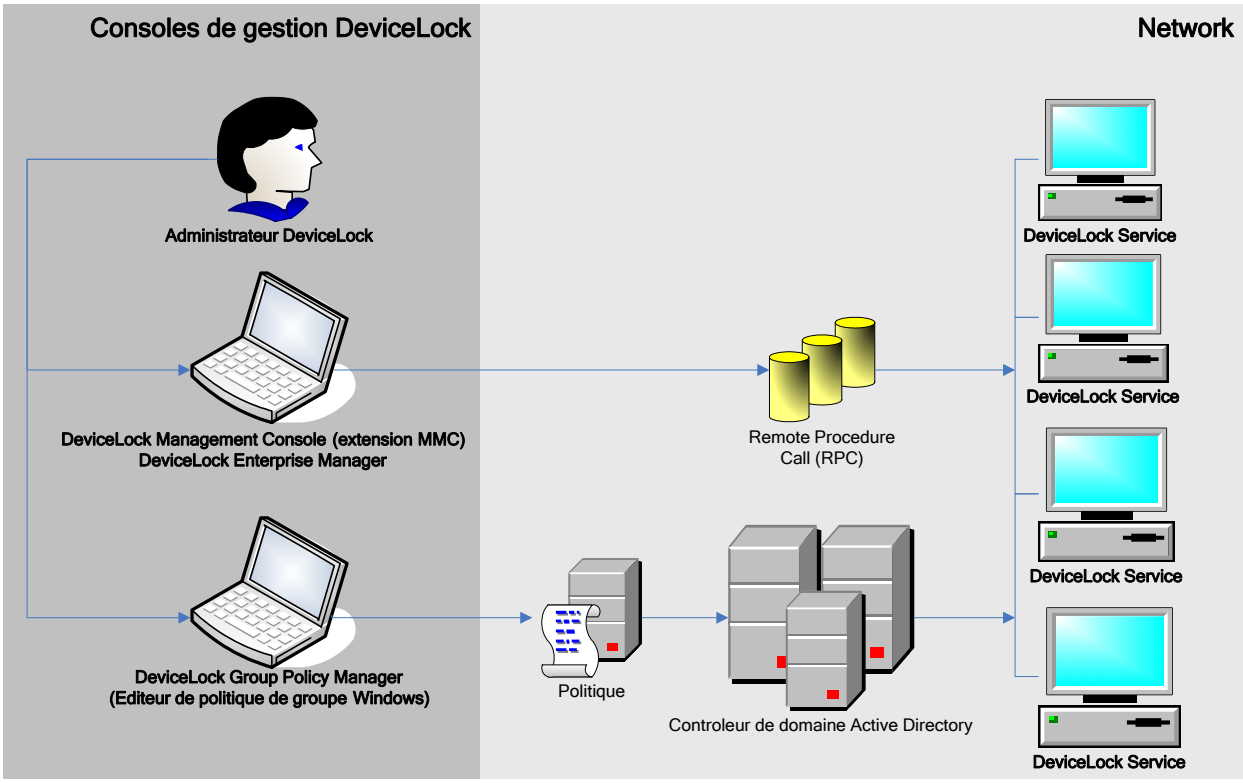


2. DeviceLock Enterprise Server est un élément optionnel destiné à la collecte et au stockage centralisé des données de réplication et des registres d'audit. DeviceLock Enterprise Server utilise MS SQL Server pour stocker les données. Vous pouvez installer plusieurs DeviceLock Entreprise Server pour partager uniformément la charge du réseau.



DeviceLock Content Security Server est un autre composant optionnel qui inclut Search Server pour la recherche instantanée de texte dans les fichiers masqués et les autres journaux stockés sur DeviceLock Enterprise Server. Pour plus d'informations, veuillez consulter la section «Comprendre DeviceLock Content Security Server.»

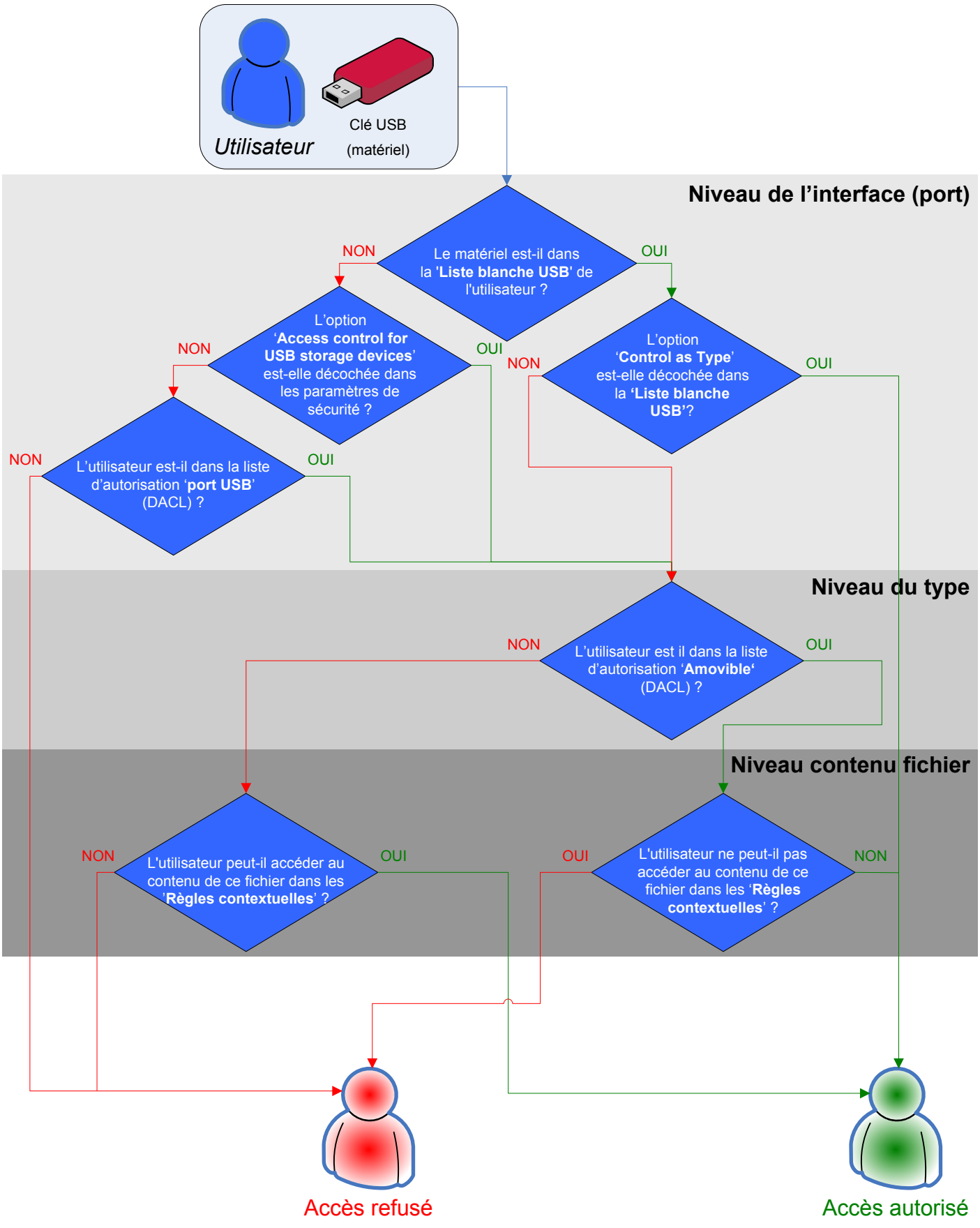
3. La console d'administration est l'interface de gestion destinée aux administrateurs systèmes soucieux de paramétrer à distance chaque système équipé de DeviceLock Service. DeviceLock est livré avec trois consoles de gestion différentes: DeviceLock Management Console (l'extension MMC), DeviceLock Enterprise Manager et DeviceLock Group Policy Manager (intégré dans l'éditeur de politique de groupe Windows). DeviceLock Management Console permet aussi de gérer DeviceLock Enterprise Server et DeviceLock Content Security Server.



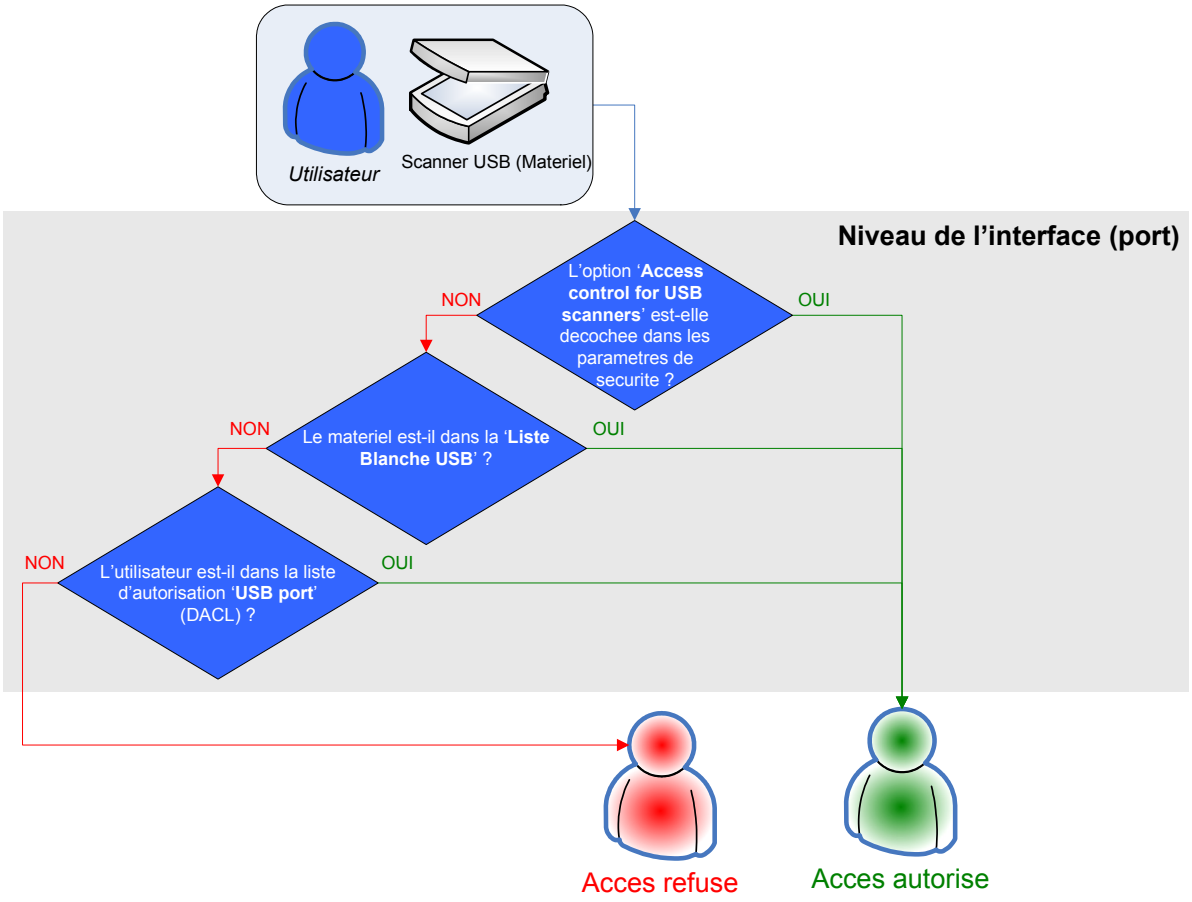
Contrôle d'accès géré aux périphériques et aux protocoles

Le contrôle d'accès aux périphériques fonctionne de la manière suivante: A chaque fois qu'un utilisateur essaie d'utiliser un périphérique, DeviceLock intercepte sa demande au niveau du noyau du système d'exploitation. Selon le type de périphérique et l'interface de connexion (USB, par exemple), DeviceLock vérifie les droits de l'utilisateur dans la liste de contrôle d'accès (ACL) appropriée. Si l'utilisateur n'a pas le droit d'accéder à ce périphérique, un message de type «accès refusé» lui est retourné.

Les accès peuvent être vérifiés à trois niveaux: au niveau de l'interface (le port), au niveau de la typologie et au niveau contextuel. Certains périphériques sont soumis à des vérifications à tous les niveaux, d'autres à un seul (au niveau de l'interface (le port) ou au niveau de la typologie).


Utilisateur
Clé USB
(matériel)
Niveau de l'interface (port)
Le matériel est-il dans la 'Liste blanche USB' de l'utilisateur ?
NON
OUI
L'option 'Access control for USB storage devices' est-elle décochée dans les paramètres de sécurité ?
NON
OUI
L'option 'Control as Type' est-elle décochée dans la 'Liste blanche USB'?
NON
OUI
L'utilisateur est-il dans la liste d'autorisation 'port USB' (DACL) ?
NON
OUI
Niveau du type
L'utilisateur est il dans la liste d'autorisation 'Amovible' (DACL) ?
NON
OUI
Niveau contenu fichier
L'utilisateur peut-il accéder au contenu de ce fichier dans les 'Règles contextuelles' ?
NON
OUI
L'utilisateur ne peut-il pas accéder au contenu de ce fichier dans les 'Règles contextuelles' ?
OUI
NON
Accès refusé
Accès autorisé

Imaginez un utilisateur qui branche sa clé USB sur un port USB. Dans ce cas, DeviceLock vérifiera d'abord si le port USB est ouvert ou verrouillé au niveau de l'interface. Ensuite, comme Windows considère qu'une clé USB est un dispositif de stockage amovible, DeviceLock vérifiera les autorisations au niveau typologique (ici de type Amovible). Enfin, DeviceLock vérifiera les autorisations au niveau contextuel (Content-Aware Rules ou règles contextuelles). En revanche, un scanner USB ne sera contrôlé qu'au niveau de l'interface (port USB) puisque DeviceLock ne considère pas les scanners comme un type de matériel en soi.



D'autres Security Settings permettent de supprimer le contrôle d'accès pour certaines classes de matériel particulières (par exemple, toutes les imprimantes USB), alors que les autres demeurent sous contrôle. Dans ce cas, si le périphérique appartient à une classe pour laquelle le contrôle d'accès a été désactivé, DeviceLock autorise systématiquement la connexion de ce périphérique au niveau de l'interface (le port).

De plus, DeviceLock prend en compte l'inscription de périphériques spécifiques sur des White Lists. Autrement dit, vous pouvez soustraire au contrôle d'accès un matériel particulier (une de vos imprimantes USB, par exemple).

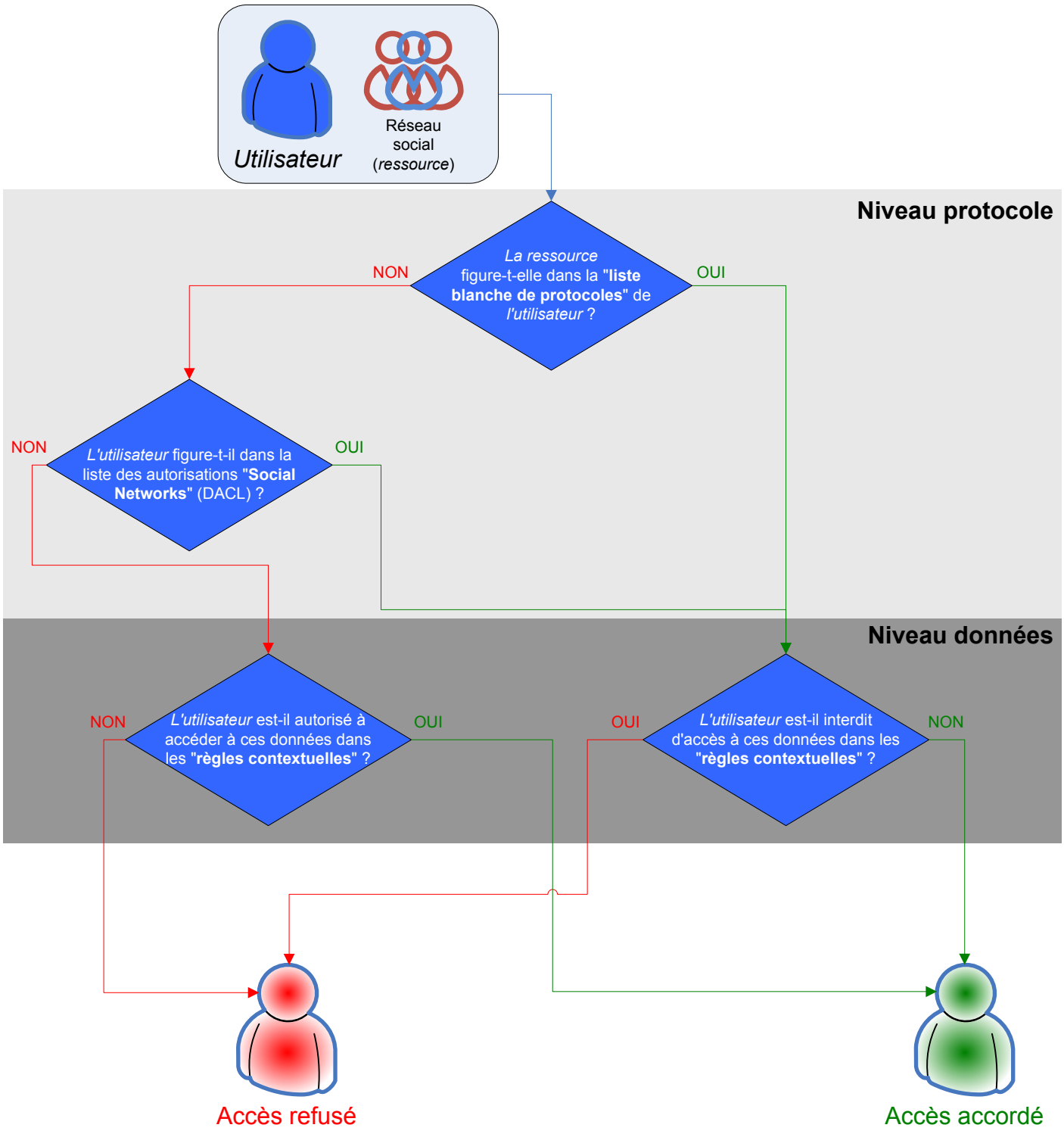
Remarque: Si l'accès à un périphérique est refusé au niveau de l'interface (le port), DeviceLock ne vérifie pas les autorisations au niveau typologique. Par contre, si l'accès est accordé au niveau de l'interface, DeviceLock vérifie aussi les autorisations au niveau typologique. Ce n'est qu'une fois l'accès accordé aux deux niveaux que l'utilisateur est à même de connecter le périphérique.

Le contrôle d'accès aux protocoles fonctionne de la manière suivante: À chaque fois qu'un utilisateur essaie d'accéder à une ressource réseau, DeviceLock intercepte sa demande au niveau du système d'exploitation et vérifie les droits de l'utilisateur dans la liste de contrôle d'accès (ACL) appropriée. Si l'utilisateur ne dispose pas des droits nécessaires pour accéder à ce protocole, un message du type «access denied» (accès refusé) lui est transmis.

Remarque: Les paramètres de contrôle d'accès aux réseaux sociaux et à la messagerie Web prévalent sur les paramètres de contrôle d'accès HTTP. Par exemple, un utilisateur disposant de droits d'accès à Gmail mais pas au protocole HTTP peut tout de même accéder au service de messagerie Web (Gmail).

Les accès peuvent être vérifiés à deux niveaux: au niveau du protocole et au niveau contextuel. Toutes les connexions réseau, à l'exception des connexions Telnet, sont vérifiées aux deux niveaux.

Prenons l'exemple d'un utilisateur se connectant à un site de réseau social. Dans ce cas, DeviceLock vérifiera d'abord si l'accès aux réseaux sociaux est ouvert ou verrouillé au niveau du protocole. Ensuite, DeviceLock vérifiera les autorisations au niveau contextuel (règles contextuelles).



De plus, DeviceLock prend en compte l'inscription des protocoles sur des listes blanches. Grâce aux listes blanches de protocoles, il est possible de supprimer le contrôle d'accès pour les connexions ayant des paramètres spécifiques (par exemple, les connexions HTTP vers des hôtes et des ports spécifiques).

Comprendre DeviceLock Content Security Server

DeviceLock Content Security Server est un nouvel élément optionnel de DeviceLock. Il inclut Search Server qui permet la recherche systématique des données de journal stockées sur DeviceLock Enterprise Server. Ces capacités de recherche permettent une gestion plus facile et plus efficace de la quantité de données toujours plus grande contenue dans les bases de données de DeviceLock Enterprise Server.

DeviceLock Content Security Server comprend les fonctions suivantes:

- **Exploration systématique de texte.** L'option Search Server de DeviceLock Content Security Server permet une recherche instantanée des textes souhaités en fonction de différents critères de recherche.
- **Options de configuration flexibles.** Différentes options de configuration sont prises en charge, d'où la possibilité d'optimiser les performances de DeviceLock Content Security Server en fonction de votre installation.

Les explorations systématiques de texte permettent de trouver des données indétectables par simple filtrage des données à l'aide des modules d'affichage de journaux. La fonction d'exploration systématique de texte est particulièrement utile dans les situations où il s'agit de rechercher des copies de réplication de documents en fonction de leurs contenus.

Exemple d'utilisation: Empêcher les fuites d'informations confidentielles
Les spécialistes sécurité chargés de veiller au caractère confidentiel des informations classées peuvent utiliser régulièrement Search Server pour trouver, récupérer et analyser de façon simple toutes les copies répliquées de fichiers contenant des données stratégiques comme des listes de clients ou de tarifs. Les données associées aux copies répliquées ainsi identifiées permettent de déterminer quand et par qui ces informations confidentielles ont été copiées. Les spécialistes sécurité peuvent ainsi prendre des mesures immédiates pour éviter une éventuelle publication de ces informations et leur diffusion en dehors de l'entreprise.

DeviceLock Content Security Server peut être configuré à l'aide de DeviceLock Management Console.

Mode de fonctionnement de Search Server

Search Server remplit les fonctions suivantes:

- Indexation des données de DeviceLock Enterprise Server.
- Recherches de textes systématiques une fois les données indexées.

Ces fonctions sont décrites de façon plus détaillée ci-dessous.

Indexation des données de DeviceLock Enterprise Server

L'indexation est un processus qui permet la recherche et la récupération de données de texte sur DeviceLock Enterprise Server.

Search Server démarre le processus d'indexation automatiquement dès que vous choisissez un ou plusieurs DeviceLock Enterprise Servers. Le processus d'indexation peut déboucher soit sur la création, soit sur la mise à jour de l'indice systématique du texte. Il n'y a qu'un seul indice systématique de texte par Search Server, d'où une gestion plus efficace. L'indice systématique de texte contient des informations sur les principaux mots et leurs emplacements. Lors de la création ou de la mise à jour de l'indice, Search Server élimine les mots inutiles (comme les prépositions, les articles, etc.) qui ne contribuent en rien à la recherche.

Search Server indexe toutes les données du texte à partir des sources de contenus suivantes: journal d'audit, journal de réplication, journal des données de réplication supprimées, journal de serveur et journal de surveillance.

Le processus d'indexation a lieu en deux étapes. Lors de la première étape, Search Server extrait les principaux mots des copies de réplication et des enregistrements de journaux, puis les enregistre dans des indices temporaires pour chacun des DeviceLock Enterprise Servers indiqués. Pour chaque indice temporaire, Search Server traite 1000 enregistrements par journal.

Lors de la deuxième étape, autrement dit une fois le nombre d'indices temporaires supérieur ou égal à 50, ou au bout de 10 minutes, tous les indices temporaires sont combinés sous forme d'indice principal permanent utilisé pour les recherches. Ce processus de consolidation des indices temporaires sous forme d'indice principal reçoit le nom de ***fusion***.

La création de l'indice principal est un processus qui prend beaucoup de temps. La vitesse d'indexation peut varier considérablement en fonction du type de données indexées et du matériel utilisé. En général, la vitesse d'indexation varie de 30 à 120 Mo/minute. En voici un exemple:

- Données: 170 Go, constitués de 4 373 004 fichiers de plusieurs types (HTML, documents office, texte)
- Temps d'indexation: 24,7 h (6,8 Go/h)
- Taille de l'indice: 12 % de la taille du document d'origine
- Matériel: Processeur 550 Pentium® 4 (3,40 GHz, 800 FSB), 2 Go RAM, disques durs internes SATA RAID-0

Explorations systématiques de texte

Une fois les données du DeviceLock Enterprise Server indexées, il est possible d'effectuer des explorations systématiques de texte. Ces recherches permettent d'identifier un ou plusieurs mots ou phrases particuliers.

Lors d'une recherche, Search Server traite la demande et récupère une liste des résultats correspondant au critère de recherche dans l'indice. Il est possible de filtrer la recherche afin de limiter le nombre de résultats affichés. Par exemple, les résultats peuvent être filtrés par journal ou par date.

L'exploration systématique de l'indice est extrêmement rapide et flexible. Une opération de recherche ne met que quelques secondes à identifier et afficher les résultats correspondant à des critères de recherche particuliers. Pour obtenir des informations détaillées sur la page des résultats de recherche et les résultats de recherche eux-mêmes, veuillez consulter la section «Utilisation des résultats de recherche.»

Extension des fonctionnalités de DeviceLock avec ContentLock et NetworkLock

DeviceLock est fourni avec ContentLock et NetworkLock, des composants sous licence séparée offrant des fonctionnalités supplémentaires à DeviceLock. Ces composants sont installés automatiquement, mais nécessitent une licence pour fonctionner. Pour plus d'informations à propos des licences ContentLock et NetworkLock, consultez le chapitre «Licences.»

NetworkLock ajoute des fonctionnalités complètes de contrôle contextuel aux terminaux de communication réseau. Il prend en charge la détection des protocoles et des applications réseau indépendants des ports et le blocage sélectif, la reconstruction des messages et des sessions avec extraction de fichiers, de données et de paramètres, ainsi que la journalisation et la réplication des données. NetworkLock contrôle les protocoles et les applications réseau les plus populaires tels que : la protection par texte clair et par SSL des communications e-mail SMTP (avec contrôle séparé des messages et des pièces jointes), les application d'accès Web et autres applications basées sur le protocole HTTP, y compris l'inspection contextuelle des sessions HTTPS cryptées (plus précisément, les applications de messagerie Web et de réseaux sociaux telles que Gmail, Yahoo! Mail, Windows Live Mail, Facebook, Twitter, LiveJournal, etc.), les applications de messagerie instantanée (ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), les protocoles de transfert de fichier sur FTP et sur FTP-SSL, ainsi que les sessions Telnet.

NetworkLock est représenté dans l'interface utilisateur de la DeviceLock Management Console, du Service Settings Editor et du DeviceLock Group Policy Manager par le nœud **Protocols**.

NetworkLock offre les principaux avantages et caractéristiques suivants:

- **Contrôle d'accès aux protocoles**. Il est possible d'appliquer aux utilisateurs ou groupes d'utilisateurs des restrictions d'accès planifié aux protocoles FTP, HTTP, SMTP, Telnet, aux messageries instantanées (ICQ, AOL, Windows Live Messenger, Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), ainsi qu'aux applications de messagerie Web et de réseaux sociaux (AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING) en fonction de l'heure du jour et du jour de la semaine.
- **Liste blanche de protocoles**. Vous pouvez accorder des permissions sélectives aux communications réseau pour les protocoles spécifiés, indépendamment des paramètres de blocage de protocoles existants. Les listes blanches sont plus efficaces dans les scénarios de «moindre privilège», lorsque tous les protocoles sont bloqués et qu'elles autorisent uniquement ceux nécessaires à l'accomplissement des tâches quotidiennes des employés.
- **Définition de règles contextuelles (détection des types de fichiers)**. Vous pouvez accorder ou refuser, de façon sélective, l'accès à certains types de fichiers transmis sur le réseau. La reconnaissance et l'identification des types de fichiers sont uniquement basées sur leur contenu. Cet algorithme efficace et fiable permet l'identification et la gestion appropriées des fichiers, indépendamment de leur extension. Les règles contextuelles permettent également d'accorder ou de refuser la copie de réplication de certains types de fichiers.

  Remarque: L'activation des capacités avancées des règles contextuelles nécessite l'achat d'une licence ContentLock.

- **Audit et Shadowing**. Cette fonctionnalité permet de suivre les activités de l'utilisateur pour les protocoles spécifiés et de créer un journal complet des données et des fichiers transmis sur le réseau.

ContentLock est un composant de surveillance et de filtrage contextuels qui améliore considérablement les capacités des règles contextuelles. Avec ContentLock, il est non seulement possible d'accorder ou de refuser l'accès aux informations sur la base des types de fichiers réels, mais aussi de créer des filtres d'expressions avec des conditions numériques et des combinaisons booléennes de critères de filtrage et de mots de passe. Capable de reconnaitre plus de quatre-vingt formats de fichiers et types de données, ContentLock extrait et filtre les données copiées sur des disques amovibles et des périphériques de stockage plug-and-play, ainsi que les données transmises sur le réseau. Avec ContentLock, vous pouvez également filtrer les données répliquées pour ne permettre que l'information strictement nécessaire à

l'audit de sécurité, aux enquêtes sur les incidents et aux analyses de protection avant sauvegarde dans le journal de réplication. Cela permet de réduire considérablement l'espace de stockage et les exigences de bande passante du réseau pour l'acheminement du journal de réplication à la base de données centrale.

ContentLock offre les principaux avantages et caractéristiques suivants:

- **Contrôle d'accès contextuel aux documents**. Vous pouvez contrôler l'accès aux documents en fonction de leur contenu. Ainsi, vous pouvez bloquer les fuites de contenus sensibles tout en accordant aux employés les droits d'accès aux informations dont ils ont besoin pour leur travail.
- **Filtrage contextuel des données de réplication**. Vous pouvez spécifier que seules les données contenant des informations sensibles soient répliquées et sauvegardées dans le journal de réplication, réduisant d'autant le volume de données de journalisation superflues et simplifiant la manipulation des fichiers journaux.
- **Prise en charge de nombreux formats de fichiers et types de données**. La protection de contenus prend en charge les formats de fichiers et les types de données suivants: Adobe Acrobat (.pdf), Adobe Framemaker MIF (.mif), Ami Pro (.sam), Ansi Text (.txt), SCII Text, fichiers multimédia ASF (métadonnées uniquement) (.asf), CSV (Comma-separated values) (.csv), DBF (.dbf), EBCDIC, fichiers EML (e-mails enregistrés par Outlook Express) (.eml), Enhanced Metafile Format (.emf), fichiers de messages Eudora MBX (.mbx), Flash (.swf), GZIP (.gz), HTML (.htm, .html), JPEG (.jpg), Lotus 1-2-3 (.123, .wk?), fichiers archivés d'e-mails MBOX (y compris Thunderbird) (.mbx), fichiers archivés MHT (Fichiers archivés HTML enregistrés par Internet Explorer) (.mht), messages MIME, fichiers MSG (e-mails enregistrés par Outlook) (.msg), fichiers Microsoft Access MDB (.mdb, .accdb, y compris Access 2007 et Access 2010), Microsoft Document Imaging (.mdi), Microsoft Excel (.xls), Microsoft Excel 2003 XML (.xml), Microsoft Excel 2007 et 2010 (.xlsx), Microsoft Outlook/Exchange Messages, Notes, Contacts, Rendez-vous et tâches, mémoire de message Microsoft Outlook Express 5 et 6 (.dbx), Microsoft PowerPoint (.ppt), Microsoft PowerPoint 2007 et 2010 (.pptx), Microsoft Rich Text Format (.rtf), Microsoft Searchable Tiff (.tiff), Microsoft Word pour DOS (.doc), Microsoft Word pour Windows (.doc), Microsoft Word 2003 XML (.xml), Microsoft Word 2007 et 2010 (.docx), Microsoft Works (.wks), MP3 (métadonnées uniquement) (.mp3), Multimate Advantage II (.dox), Multimate version 4 (.doc), documents, feuilles de calcul et présentations OpenOffice versions 1, 2 et 3 (.sxc, .sxd, .sxi, .sxw, .sxg, .stc, .sti, .stw, .stm, .odt, .ott, .odg, .otg, .odp, .otp, .ods, .ots, .odf) (y compris OASIS Open Document Format for Office Applications), Quattro Pro (.wb1, .wb2, .wb3, .qpw), QuickTime (.mov, .m4a, .m4v), TAR (.tar), TIFF (.tif), TNEF (fichiers winmail.dat), fichiers Treepad HJT (.hjt), Unicode (UCS16, ordre des octets Mac ou Windows, ou UTF-8), fichiers Visio XML (.vdx), Windows Metafile Format (.wmf), fichiers multimédia WMA (métadonnées

uniquement) (.wma), fivhiers vidéo WMV (métadonnées uniquement) (.wmv), WordPerfect 4.2 (.wpd, .wpf), WordPerfect (5.0 et supérieur) (.wpd, .wpf), WordStar version 1, 2, 3 (.ws), WordStar versions 4, 5, 6 (.ws), WordStar 2000, Write (.wri), XBase (y compris FoxPro, dBaseet autres formats compatibles XBase) (.dbf), XML (.xml), XML Paper Specification (.xps), XSL, XyWrite, ZIP (.zip).

- **Protection automatique des nouveaux documents**. Vous pouvez configurer des politiques de sécurité contextuelle s'appliquant aux nouveaux documents dès leur création.
- **De nombreuses méthodes de détection de contenu**. Vous disposez de plusieurs méthodes pour identifier le contenu des documents (basées sur la fréquence des termes, sur des mots clés et sur les propriétés du document).
- **Gestion centralisée de contenu**. Les règles contextuelles sont créées sur la base de groupes de contenus permettant de définir, de façon centralisée, les types de contenus pour lesquels vous désirez appliquer des restrictions d'accès.
- **Possibilité d'outrepasser les politiques de contrôle d'accès au typologique ou au niveau du protocole**. Vous pouvez accorder ou refuser, de manière sélective, l'accès à certains contenus, indépendamment des permissions préétablies au niveau typologique ou au niveau du protocole.
- **Inspection des fichiers dans les archives**. Cette fonctionnalité permet d'effectuer une inspection en profondeur de chaque fichier individuel contenu dans une archive. L'algorithme d'inspection suivant est utilisé: Lorsqu'un utilisateur essaie de copier un fichier archivé vers un périphérique ou de le transmettre sur le réseau, tous les fichiers contenus dans l'archive sont extraits et analysés séparément afin de déterminer les contenus auxquels les règles contextuelles restreignent l'accès. Si l'accès à au moins un des fichiers extraits de l'archive est restreint pour cet utilisateur, l'accès à l'archive lui sera également refusé. Si l'accès à au moins un des fichiers extraits de l'archive est restreint pour cet utilisateur, l'accès à l'archive lui sera également refusé. Tous les fichiers archivés sont extraits dans le dossier temporaire (Temp) de l'utilisateur System. En général, le dossier temporaire (Temp) se trouve à l'adresse suivante: répertoire %windir%\Temp. Si DeviceLock Service n'a pas accès au dossier Temp, les fichiers archivés ne seront pas analysés. L'accès à l'archive n'est alors refusé que dans l'un des cas suivants:
    - Il existe une règle de refus contextuel (Deny Content-Aware Rule)
    - Les permissions établies au niveau typologique ou au niveau du protocole restreignent l'accès

  Toutes les archives imbriquées sont également décompressées et analysées individuellement. La détection des fichiers archivés se fait sur la base de leur contenu, et non de leur extension. Les formats d'archives suivants sont pris en charge: 7z (.7z), ZIP (.zip), GZIP (.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar), LZMA (.lzma), RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm,

.chw, .hxs), ISO (.Iso), UDF (.Iso), COMPOUND (.Msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe). Les archives en plusieurs parties (multi volumes) et les archives protégées par mots de passe ne sont pas décompressées.

- **Détection du texte sur les images**. L'utilisation de la technologie de détection de texte sur des images permet de classer toutes les images en deux groupes: les images à texte (images contenant du texte, telles que des documents scannés, des captures d'écran) et les images sans texte (images ne contenant pas de texte). Ainsi, le contrôle d'accès peut se faire séparément pour chaque groupe. À titre d'exemple, vous pouvez permettre aux utilisateurs de copier des images sans texte vers des périphériques, mais leur restreindre l'accès aux images à texte, évitant ainsi de potentielles fuites d'informations sensibles provenant des fichiers d'images. Les fichiers d'images suivants sont pris en charge: fichiers BMP, fichiers Dr. Halo CUT, fichiers DDS, fichiers EXR, fichiers Raw Fax G3, fichiers GIF, fichiers HDR, fichiers ICO, fichiers IFF (à l'exception des fichiers Maya IFF), fichiers JBIG, fichiers JNG, fichiers JPEG/JIF, format de fichier JPEG-2000, JPEG-2000 codestream; fichiers KOALA, fichiers Kodak PhotoCD, fichiers MNG, fichiers PCX, fichiers PBM/PGM/PPM, fichiers PFM, fichiers PNG, fichiers Macintosh PICT, fichiers Photoshop PSD, fichiers Camera RAW, fichiers Sun RAS, fichiers SGI, fichiers TARGA, fichiers TIFF, fichiers WBMP, fichiers XBM, fichiers XPM.
- **Inspection des images intégrées dans des documents**. Cette fonctionnalité permet d'effectuer une inspection poussée de chaque image individuelle incorporée dans les fichiers Adobe Portable Document Format (PDF), ainsi que dans les documents Rich Text Format (RTF) et Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx). Toutes les images incorporées sont extraites de ces documents vers le dossier Temp de l'utilisateur System et analysées indépendamment du texte de leur document d'origine, afin de déterminer les contenus auxquels les règles contextuelles restreignent l'accès. Des règles contextuelles, créées d'après des mots clés, des filtres ou des groupes de contenus complexes, effectuent une vérification du texte contenu dans les documents. D'autres règles contextuelles, créées d'après la détection de type de fichier, les propriétés du document ou des groupes de contenus complexes, effectuent une vérification des images incorporées dans les documents. L'accès aux documents n'est accordé que lorsque les règles contextuelles permettent l'accès à la fois au texte et aux images contenus dans ces documents.

Licences

L'utilisation des capacités de NetworkLock et de ContentLock nécessite l'achat des licences NetworkLock et ContentLock, en plus des licences DeviceLock de base. Une licence NetworkLock permet d'utiliser la fonctionnalité Protocols. Une licence ContentLock active la fonctionnalité de création et l'utilisation des règles contextuelles basées sur la fréquence des termes et expressions, sur des mots clés

et sur les propriétés des documents, ainsi que sur des règles plus complexes intégrant des combinaisons booléennes et des critères de filtrage.

Si vous utilisez des licences de types différents, veuillez prendre en compte les éléments suivants:

- Si vous possédez une licence DeviceLock de base, une licence ContentLock et une licence Network, vous pouvez utiliser la fonctionnalité Protocols, créer et utiliser des règles contextuelles basées sur les types de fichiers, sur la fréquence des termes et expressions, sur des mots clés et sur les propriétés des documents, ainsi que sur des règles plus complexes.
- Si vous possédez uniquement une licence DeviceLock de base, vous ne pouvez pas utiliser la fonctionnalité Protocols, ni créer ou utiliser des règles contextuelles basées sur la fréquence des termes et expressions, sur des mots clés et sur les propriétés des documents, ainsi que sur des règles plus complexes. Par contre, vous pouvez créer et utiliser des règles contextuelles basées sur les types de fichiers (détection de type de fichier).
- Si vous possédez une licence DeviceLock de base et une licence ContentLock, vous pouvez créer et utiliser des règles contextuelles basées sur les types de fichiers, sur la fréquence des termes et expressions, sur des mots clés et sur les propriétés des documents, ainsi que sur des règles plus complexes. Mais vous ne pouvez pas utiliser la fonctionnalité Protocols.
- Si vous possédez une licence DeviceLock de base et une licence Network, vous pouvez utiliser la fonctionnalité Protocols, créer et utiliser des règles contextuelles basées sur les types de fichiers. Mais vous ne pouvez ni créer, ni utiliser des règles contextuelles basées sur la fréquence des termes et expressions, sur des mots clés et sur les propriétés des documents, ainsi que sur des règles plus complexes.
- Une licence DeviceLock de base est obligatoire, tandis que les licences NetworkLock et ContentLock sont optionnelles. En cas d’absence ou d’invalidité d’une licence de base, DeviceLock fonctionnera uniquement en mode essai. Le nombre de licences NetworkLock et/ou ContentLock doit être au moins égal au nombre de licences DeviceLock de base.
- La période d’essai pour les licences ContentLock et NetworkLock est de 30 jours.

Mesures de sécurité de base recommandées

Vous trouverez ci-dessous une série de recommandation de sécurité de base que doivent observer tous les ordinateurs installés sur un réseau d’entreprise :

- ***Changement de la séquence de démarrage.*** Le disque dur doit être le premier périphérique de démarrage. Changez la séquence de démarrage dans le BIOS afin d'éviter que l'ordinateur ne démarre à partir de la disquette, du

lecteur USB ou du CD-ROM. Si le disque dur n'est pas le premier périphérique de démarrage, quelqu'un peut utiliser un CD ou une clé USB de démarrage pour accéder directement au disque dur.

- ***Protection du BIOS par un mot de passe.*** Le BIOS doit comporter un mot de passe afin d'empêcher les personnes non autorisées d'y apporter des modifications. Dans le cas contraire, quelqu'un peut modifier la séquence de démarrage et utiliser un CD, une disquette ou une clé USB de démarrage (voir ci-dessus).
- ***Scellée des boîtiers et des châssis d'ordinateurs.*** Protégez le matériel à l'aide de scellées. Sinon, il est possible de brancher un périphérique de démarrage externe directement sur l'ordinateur et d'accéder au disque dur. Qui plus est, si vous laissez quelqu'un accéder physiquement à la carte mère, il lui est très facile de localiser le cavalier de réinitialisation de la mémoire CMOS et d'effacer le mot de passe du BIOS (voir ci-dessus).
- ***Refus de droits d'administrateur aux utilisateurs habituels.*** Les utilisateurs locaux ne doivent pas faire partie du groupe local des administrateurs. Il est déconseillé d'accorder aux utilisateurs le droit d'administrer leurs ordinateurs.

  Cependant, si pour une raison ou pour une autre, des utilisateurs de votre réseau possèdent des privilèges d'administrateur sur leurs ordinateurs locaux, DeviceLock comporte un autre niveau de protection. Personne, hormis les administrateurs DeviceLock autorisés, ne peut se connecter, interrompre ou désinstaller DeviceLock Service. Même les membres du groupe local des administrateurs sont incapables de désactiver DeviceLock s'ils ne figurent pas dans la liste des administrateurs DeviceLock autorisés.

- ***Suppression de la console de récupération.*** Si la console de récupération Windows est installée sur l'ordinateur local, quelqu'un peut démarrer en mode de récupération et déjouer n'importe quelle mesure de sécurité, y compris désactiver DeviceLock Service (même s'il faut pour cela disposer du mot de passe d'administrateur local).

  C'est pourquoi nous conseillons de supprimer la console de récupération. Pour en savoir plus sur la façon d'installer, de supprimer et d'utiliser la console de récupération, reportez-vous à l'article correspondant de l'aide en ligne Microsoft http://support.microsoft.com/default.aspx?scid=kb;fr;307654.

Installation

Prérequis

DeviceLock fonctionne sur tout ordinateur équipé de Windows NT 4.0 SP6/2000/XP/Vista/7 et Windows Server 2003/2008. Il est compatible avec les plates-formes 32 et 64 bit. Windows Internet Explorer version 4.0 ou ultérieure doit être installé sur les ordinateurs sous Windows NT 4.0 SP 6.

Remarque: Le composant NetworkLock inclus dans DeviceLock ne fonctionne pas sur les ordinateurs opérant sous Windows NT 4.0 SP 6.

Pour installer et utiliser DeviceLock, vous DEVEZ disposer de privilèges d'administration. Si vous voulez utiliser DeviceLock sur un ordinateur local, vous DEVEZ disposer de privilèges d'administration locale. Si vous envisagez d'utiliser DeviceLock sur l'ensemble de votre réseau, vous DEVEZ disposer de privilèges d'administration de domaine.

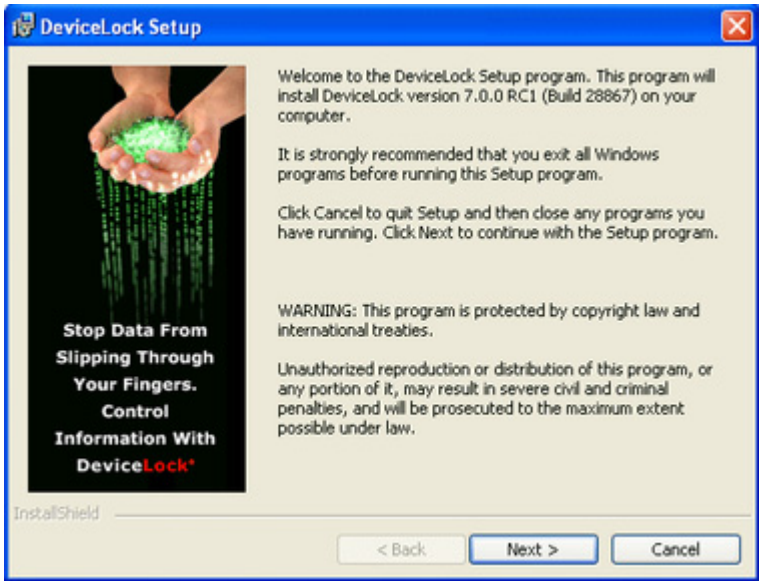
Si vous voulez utiliser DeviceLock dans votre réseau, vous DEVEZ disposer d'un protocole réseau TCP/IP actif. Cependant, DeviceLock peut aussi fonctionner sur des ordinateurs autonomes. Un réseau n'est requis que pour contrôler DeviceLock Service à partir d'un ordinateur à distance.

Déploiement de DeviceLock Service

DeviceLock Service doit être installé sur l'ordinateur pour pouvoir contrôler l'accès à ses périphériques. Il y a plusieurs manières de déployer DeviceLock sur les systèmes clients.

Installation interactive

Exécutez le programme de configuration (**setup.exe**) et suivez les instructions qui apparaissent à l'écran.


DeviceLock Setup
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
InstallShield
< Back
Next >
Cancel

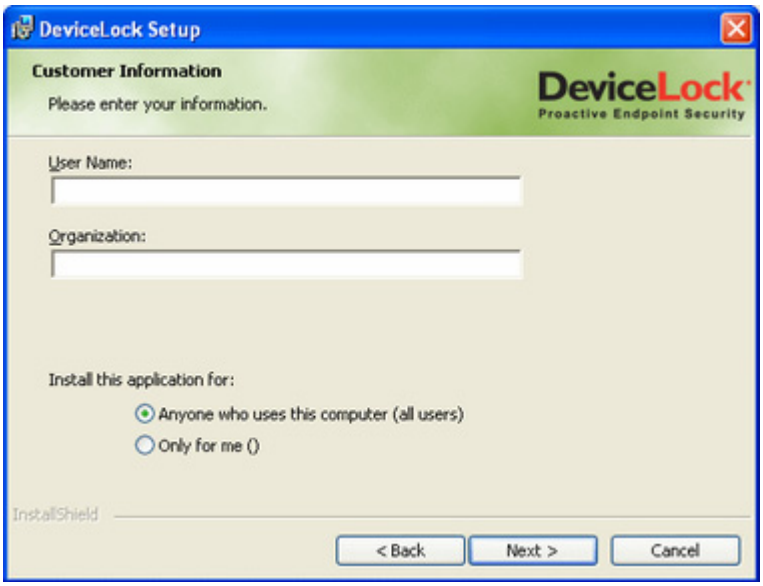
Il vous faudra exécuter **setup.exe** sur chaque ordinateur à contrôler à l'aide de DeviceLock.

Si vous effectuez une mise à jour à partir d'une ancienne version, assurez-vous d'avoir un accès administrateur à DeviceLock Service; dans le cas contraire, vous ne pourrez pas terminer l'installation.

Vous devez accepter le Contrat de licence d'utilisateur final de DeviceLock pour continuer la procédure d'installation.

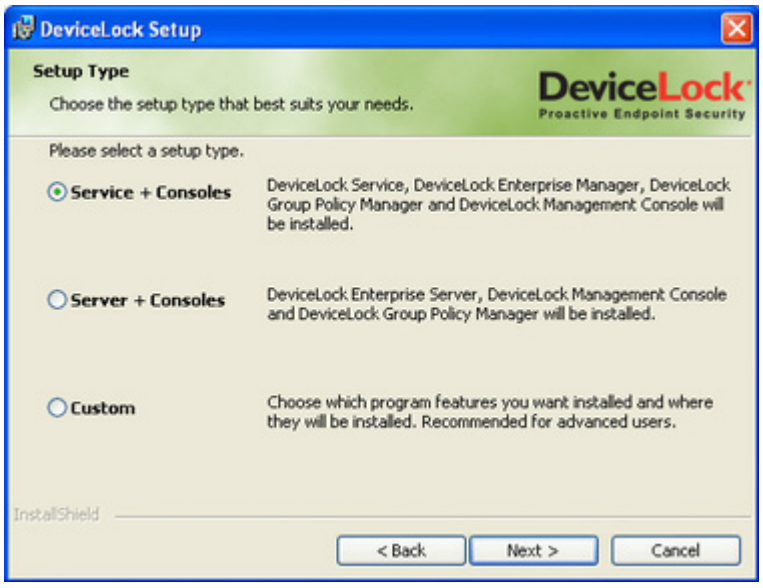
Dans la page **Customer Information** (informations du client), saisissez votre nom d'utilisateur et celui de votre organisation. Dans cette même page, sous **Install this application for** (installer cette application pour), vous pouvez indiquer les utilisateurs pour lesquels des raccourcis bureau vers les consoles de gestion DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager et DeviceLock Service Settings Editor) seront créés. Vous pouvez sélectionner l'une ou l'autre des options suivantes:

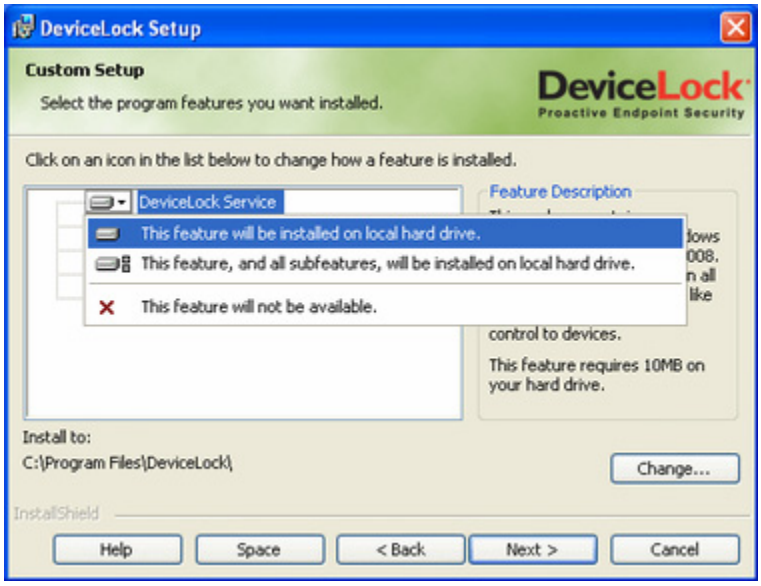
- **Anyone who uses this computer (all users)** (tous les utilisateurs): crée des raccourcis bureau vers les consoles de gestion DeviceLock pour tous les utilisateurs.
- **Only for me** (pour moi uniquement): crée des raccourcis bureau vers les consoles de gestion DeviceLock uniquement pour le compte d'utilisateur effectuant l'installation de DeviceLock.



Dans la page **Setup type** (type de configuration), sélectionnez le type de configuration requis.

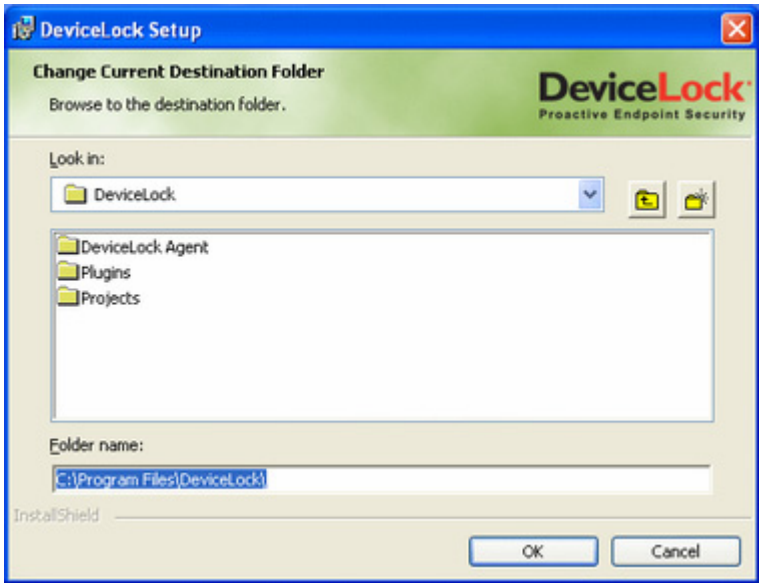
Vous pouvez, au choix: opter pour l'installation conjuguée de DeviceLock Service et DeviceLock Manager en utilisant la configuration **Services + Consoles**, ou choisir d'installer seulement DeviceLock Service en utilisant la configuration personnalisée (cochez **Custom** et sélectionnez la composante **DeviceLock Service**).


DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

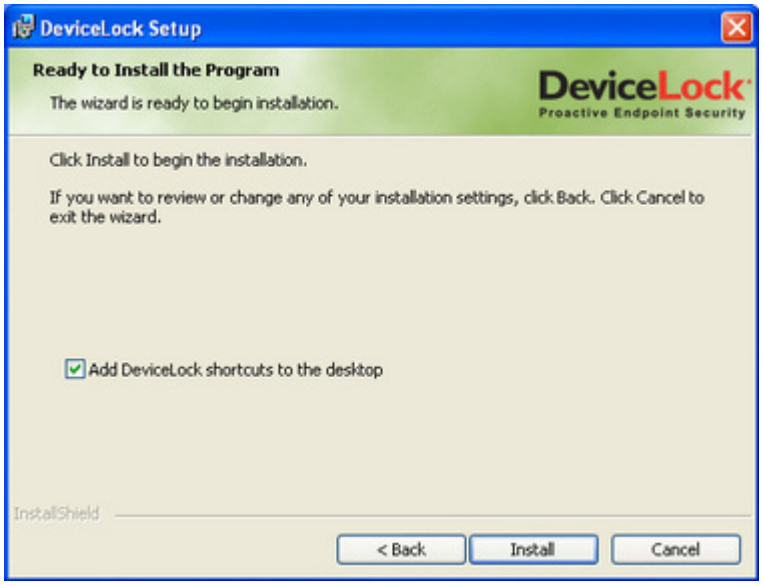

DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
Feature Description
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
control to devices.
This feature requires 10MB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Remarque: Dans la page **Custom Setup** (configuration personnalisée), choisissez le composant RSoP à installer. Ce composant active l'assistance pour le mode de planification de DeviceLock's Resultant Set of Policy sur les contrôleurs de domaine. Le composant RSoP n'est nécessaire que lorsque les consoles de gestion DeviceLock sont installées sur l'ordinateur, mais pas DeviceLock Service. Pour plus d'informations sur le mode de planification RSoP, visitez la page Microsoft documentation.

Dans la page **Custom Setup**, vous pouvez changer le répertoire d'installation par défaut. Le répertoire d'installation par défaut de DeviceLock est **%ProgramFiles%\DeviceLock**. Pour changer le répertoire d'installation, cliquez sur **Change** pour accéder à la page **Change Current Destination Folder** (répertoire d'installation actuel) et effectuer les modifications nécessaires.



Dans la page **Ready to Install the Program** (prêt pour l'installation), cliquez sur **Install** pour démarrer l'installation. Cochez la case **Add DeviceLock shortcuts to the desktop** si vous désirez créer des raccourcis vers DeviceLock Management Console (le module MMC), DeviceLock Enterprise Manager et DeviceLock Service Settings Editor sur le bureau.

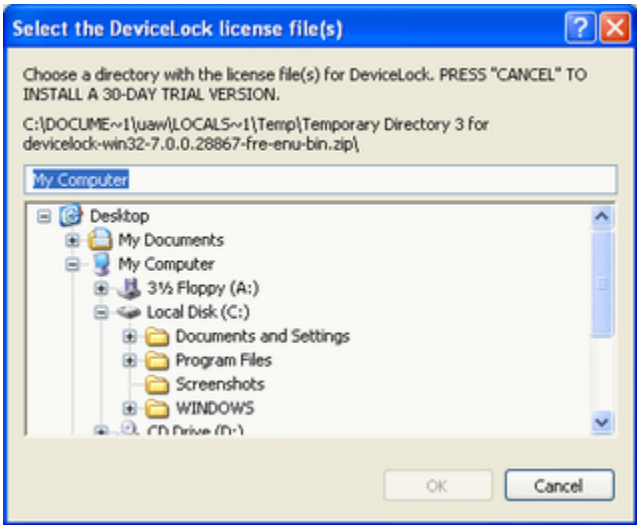

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Si vous choisissez d'installer aussi les consoles de gestion de DeviceLock, le programme risque de vous proposer de créer un nouveau DeviceLock Certificate.

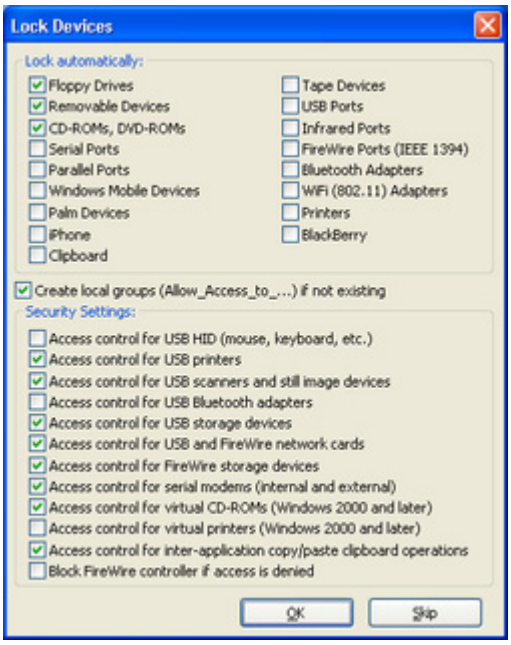
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

Vous pourrez toujours créer un nouveau certificat plus tard, en utilisant l'outil de création de certificat installé avec les consoles de gestion de DeviceLock. Par conséquent, si à ce stade vous ne savez pas si vous avez besoin du nouveau certificat, il vous suffit de cliquer sur **No** pour continuer l'installation. Pour des informations détaillées sur les DeviceLock Certificates, consultez le chapitre «DeviceLock Certificates.»

En outre, si vous sélectionnez **Service + Consoles**, l'assistant d'installation pourra vous proposer de charger les fichiers de licence DeviceLock. Si vous n'avez pas de fichier de licence, cliquez sur le bouton **Cancel** pour installer DeviceLock en mode essai de trente jours.



Pendant l'installation, vous pouvez définir des autorisations spéciales pour les périphériques locaux.



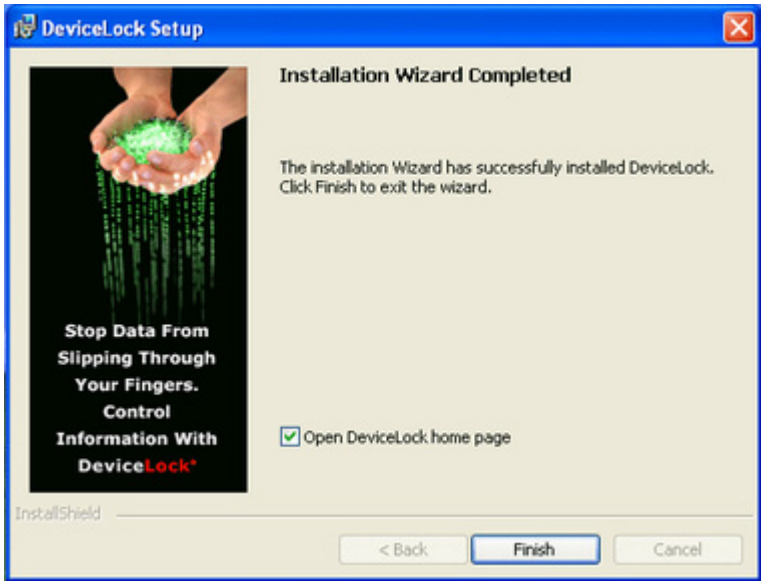
Cochez les périphériques pour lesquels vous souhaitez définir des autorisations. Cochez **Create local groups if not existing**, et le programme de configuration créera le groupe d'utilisateurs spéciaux Allow_Access_To_ pour chaque type de périphériques (p. ex. Allow_Access_To_Floppy pour les lecteurs de disquettes) si ceux-ci n'existent pas sur l'ordinateur local.

Le programme de configuration assigne les droits génériques Read, Write, Format et Eject aux membres du groupe Administrators et du compte SYSTEM. Les membres du groupe Allow_Access_To_ disposeront des droits génériques Read, Write et Eject.

Vous pouvez aussi définir des Security Settings afin d'exclure certains types de périphériques de la vérification d'accès. Pour permettre à DeviceLock Service le contrôle d'accès aux périphériques d'entrées utilisateurs (souris, clavier, etc.), les imprimantes, les scanners et les appareils d'images fixes, adaptateurs Bluetooth ou périphériques de stockage (tels que les lecteurs flash) branchés sur un port USB, cochez: **Access control for USB HID**, **Access control for USB printers**, **Access control for USB scanners and still image devices**, **Access control for USB Bluetooth adapters** ou **Access control for USB storage devices**. Pour permettre le contrôle d'accès aux cartes réseaux USB et FireWire, cochez **Access control for USB and FireWire network cards**. Sinon, même si les ports (USB et FireWire) sont verrouillés, ces périphériques continueront à fonctionner normalement. Pour permettre le contrôle d'accès à des modems en série (internes et/ou externes), cochez **Access control for serial modems**. Pour désactiver le verrouillage des CD-ROM virtuels (émulations virtuelles) sous Windows 2000 ou suivant, décochez **Access control for virtual CD-ROMs**. Pour désactiver le verrouillage des CD-ROM virtuels (émulations virtuelles) sous Windows 2000 ou suivant, décochez **Access control for virtual CD-ROMs**. Pour désactiver le contrôle des imprimantes virtuelles (celles qui impriment dans des fichiers) sur les systèmes Windows 2000 et postérieurs, décochez **Access control for virtual printers**. Pour permettre le contrôle d'accès aux opérations de copier/coller entre différentes applications, cochez la case **Access control for inter-application copy/paste clipboard operations**. À défaut, le contrôle d'accès aux opérations de copier/coller entre différentes applications sera désactivé, même si ce dernier est verrouillé. Pour désactiver les contrôleurs FireWire lorsque le compte Tous ne possède pas les permissions d'accès pour le type de périphérique port FireWire, sélectionnez la case **Block FireWire controller if access is denied**.

Pour valider les changements, cliquez sur **OK**. Cliquez sur **Skip** si vous préférez attendre la fin de l'installation pour configurer les autorisations d'accès à vos périphériques en utilisant les consoles de gestion de DeviceLock.

Dès que le programme de configuration a terminé l'installation de DeviceLock, il vous propose de visiter le site Web de DeviceLock.



Décochez la case **Open DeviceLock home page** si vous ne désirez pas visiter le site Web de DeviceLock. Cliquez sur le bouton **Finish** pour terminer l'installation.

Remarque: Pour désinstaller DeviceLock, effectuer l'une ou l'autre des actions suivantes:

Utilisez l'option **Ajouter ou supprimer des programmes** du panneau de commande pour supprimer **DeviceLock**.
- OU -
Cliquez sur **Démarrer**, sélectionnez **Tous les programmes**, puis **DeviceLock**, et cliquez sur **Remove DeviceLock**.

Installation automatique

DeviceLock Service permet aussi les installations automatiques (sans intervention humaine). On peut faire appel à ce mode d'installation dans le cas d'un fichier séquentiel. Pour installer DeviceLock Service sans intervention humaine, lancez Setup avec le paramètre **/s** (ex: **c:\setup.exe /s**). Il existe un fichier de configuration spécifique pour les configurations silencieuses, dénommé ***devicelock.ini***. Devicelock.ini doit se trouver dans le même répertoire que setup.exe. Ce fichier permet de personnaliser vos paramètres d'installation.

Devicelock.ini peut être ouvert et édité avec n'importe quel éditeur de texte, Notepad par exemple. Supprimez le point-virgule (;) situé devant le paramètre pour lui assigner une nouvelle valeur ou conservez-le pour assigner la valeur par défaut au paramètre.

Ce fichier de configuration comporte deux sections (**[Install]** et **[Misc]**), et chaque section a ses propres paramètres.

1. [Install]

Pour installer DeviceLock Service, spécifiez le paramètre **Service**.

Service = 1

Vous pouvez aussi installer les consoles de gestion DeviceLock et la documentation, en utilisant les paramètres **Manager** et **Documents**.

Pour une simple mise à jour de DeviceLock Service sans changer la configuration existante, utilisez le paramètre **OnlyUpgradeService**:

OnlyUpgradeService = 1

Dans ce cas, Setup ignore tous les paramètres spécifiés et se contente de mettre à niveau DeviceLock Service en fonction de la nouvelle version.

Vous pouvez aussi spécifier dans quel répertoire enregistrer DeviceLock:

InstallDir = C:\Program Files\DeviceLock

Le programme de configuration utilise ce répertoire s'il ne trouve pas l'installation précédente de DeviceLock.

Si vous avez acheté des licences DeviceLock, vous pouvez également préciser le répertoire de stockage des fichiers de licence:

RegFileDir = *C:\Directory*

C:\Directory étant le chemin du répertoire où se trouvent vos clés de licence.

Il est inutile de charger les licences si vous n'installez que DeviceLock Service. Elles sont nécessaires pour les consoles de gestion DeviceLock et les composants sous licence séparée: ContentLock et NetworkLock.

Pour que DeviceLock Service utilise un port fixe, spécifiez le paramètre **FixedPort** en conséquence:

FixedPort = *[numéro du port]*

Où le *numéro de port* représente le numéro du port fixe TCP que vous voulez utiliser pour les communications entre DeviceLock Service et les consoles de gestion. Pour utiliser des ports dynamiques pour la communication RPC, utilisez le numéro de port 0. Par défaut, DeviceLock Service utilise le port 9132.

Si le paramètre **CreateGroups** a pour valeur 1, le programme de configuration crée un groupe d'utilisateurs local Allow_Access_To_ spécial pour chaque type de

périphérique (ex: Allow_Access_To_Floppy pour les disquettes), si ces groupes n'existent pas sur l'ordinateur local.

Pour appliquer les paramètres, les autorisations, les règles d'audit et de réplication à DeviceLock Service, renseignez le chemin d'accès au fichier XML enregistré précédemment dans les paramètres **SettingsFile**:

SettingsFile = C:\settings.dls

Le fichier de paramètres peut être créé à l'aide de DeviceLock Management Console, de DeviceLock Group Policy Manager et/ou de DeviceLock Service Settings Editor.

2. [Misc]

Une fois l'installation réussie, pour lancer un programme (un fichier séquentiel, par exemple), spécifiez le paramètre **Run**:

Run = *C:\mybatchfile.bat*

Pour supprimer un redémarrage automatique, même si le programme de configuration en a besoin, attribuez la valeur 1 au paramètre **DisableRestart**.

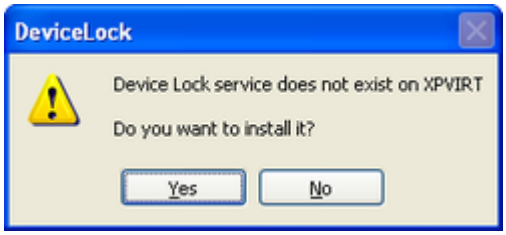
Installation via Microsoft Systems Management Server

L'installation automatique permet d'installer DeviceLock Service à l'aide du Microsoft Systems Management Server (SMS). Dans ce cas, utilisez les fichiers de définition du progiciel (DevLock.pdf pour SMS version 1.x et DevLock.sms pour SMS version 2.0 ou ultérieure) fournis avec DeviceLock, qui se trouvent dans le fichier sms.zip.

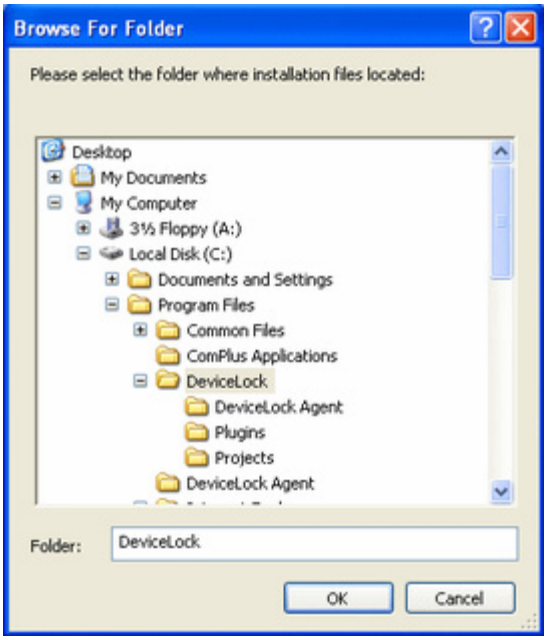
Installation à distance via DeviceLock Management Console

DeviceLock Management Console (le module MMC) prend en charge les installations à distance et permet ainsi aux administrateurs système de configurer un service sur des machines distantes sans présence physique de leur part.

Lorsque vous essayez de vous connecter à un ordinateur sur lequel DeviceLock Service n'est pas installé ou n'est pas à jour, la console de gestion vous propose de l'installer ou de le mettre à jour.



Sélectionnez le répertoire contenant tous les fichiers nécessaires à l'installation (tels que DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe et InstMsiW.exe).

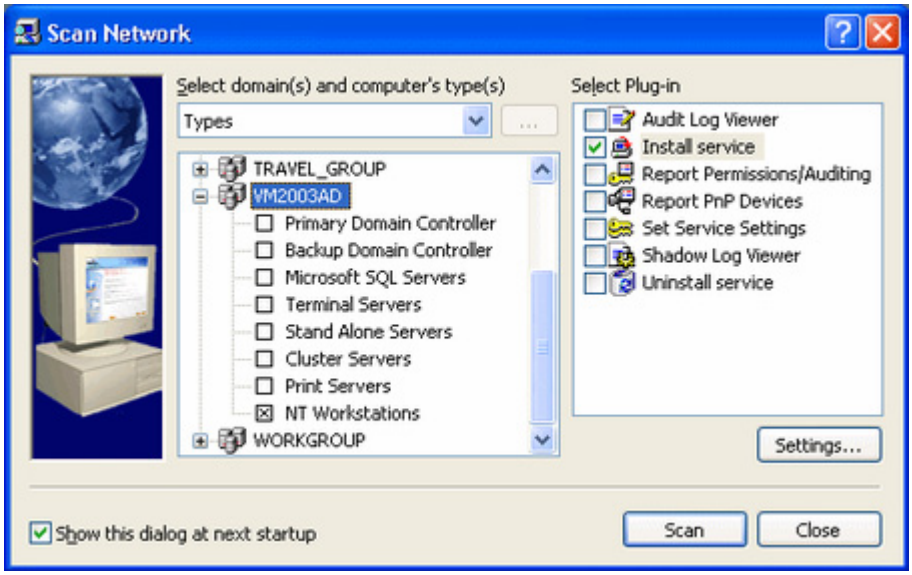


Ces fichiers se trouvent dans le répertoire d'installation de DeviceLock. Le répertoire d'installation par défaut de DeviceLock est **%ProgramFiles%\DeviceLock**.

Par défaut, les fichiers d'installation de DeviceLock Service seront copiés dans le répertoire %ProgramFiles%\DeviceLock Agent si ce service n'existe pas déjà sur le système. Si le service existe déjà sur ce système, mais dans une version antérieure à la version 7.0, la console de gestion copiera également les fichiers d'installation dans le répertoire par défaut %ProgramFiles%\DeviceLock Agent. Si le service existe sur ce système mais dans une version postérieure à la version 7.0, la console de gestion copiera le fichier d'exécution dans le répertoire de l'ancienne version et les anciens fichiers seront remplacés.

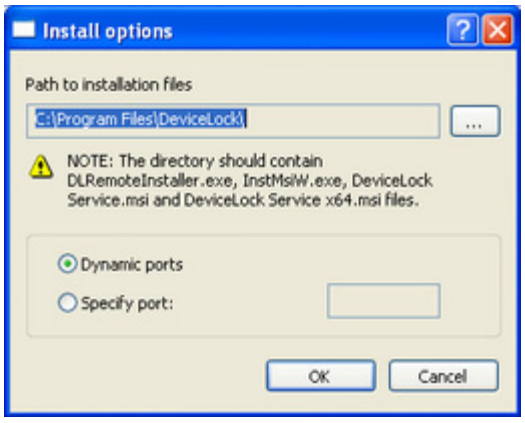
Installation à distance via DeviceLock Enterprise Manager

DeviceLock Enterprise Manager est livré avec l'extension Install service qui permet de déployer DeviceLock Service automatiquement sur tous les ordinateurs voulus de votre réseau.



Commencez par sélectionner les ordinateurs où vous souhaitez installer DeviceLock Service. DeviceLock Enterprise Manager permet une sélection par type et par nom. Vous pouvez aussi charger la liste d'ordinateurs à partir d'un fichier externe ou les sélectionner dans n'importe quelle arborescence LDAP (Active Directory, Novell eDictionary, Open LDAP, etc.).

Sélectionnez le plug-in **Install service** et cliquez sur le bouton **Settings** pour spécifier le répertoire contenant tous les fichiers nécessaires à l'installation (tels que DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe et InstMsiW.exe). Ces fichiers se trouvent dans le répertoire d'installation de DeviceLock. Le répertoire d'installation par défaut de DeviceLock est **%ProgramFiles%\DeviceLock**. Vous pouvez aussi configurer DeviceLock Service pour qu'il utilise le port TCP fixe pour communiquer avec les consoles de gestion. Pour utiliser les ports dynamiques pour la communication RPC, cliquez sur **Dynamic ports**. Par défaut, DeviceLock Service utilise le port 9132.



Par défaut, les fichiers d'installation de DeviceLock Service seront copiés dans le répertoire %ProgramFiles%\DeviceLock Agent si ce service n'existe pas déjà sur le

système. Si le service existe déjà sur ce système, mais dans une version antérieure à la version 7.0, le plug-in «Install service» copiera également les fichiers d'installation dans le répertoire par défaut %ProgramFiles%\DeviceLock Agent. Si le service existe sur ce système mais dans une version supérieure à la version 7.0, le plug-in «Install service» copiera les fichiers d'installation dans le répertoire de la version précédemment installée et remplacera les anciens fichiers.

Installation via Group Policy

Les instructions détaillées suivantes décrivent comment utiliser la politique de groupe pour distribuer automatiquement DeviceLock Service aux ordinateurs clients. DeviceLock Service peut être déployé dans un domaine Active Directory à l'aide du programme Microsoft Software Installer (MSI) (DeviceLock Service.msi et DeviceLock Service x64.msi).

Remarque: L'installation automatique de programmes via la politique de groupe de Microsoft Windows requiert des ordinateurs clients fonctionnant sous Windows 2000 ou suivants.

Si vous utilisez un progiciel MSI personnalisé avec les paramètres définis par DeviceLock Service afin de déployer DeviceLock Service en utilisant la politique de groupe, ces paramètres ne sont pas appliqués aux ordinateurs clients si l'une des conditions suivantes est remplie:

- La sécurité par défaut est désactivée sur l'exécution des DeviceLock Service distants.

- La politique de groupe GPO appliquée aux ordinateurs clients a le paramètre **Override Local Policy** activé.

Pour de plus amples informations sur la façon de créer un progiciel MSI personnalisé, veuillez consulter "Create MSI Package."

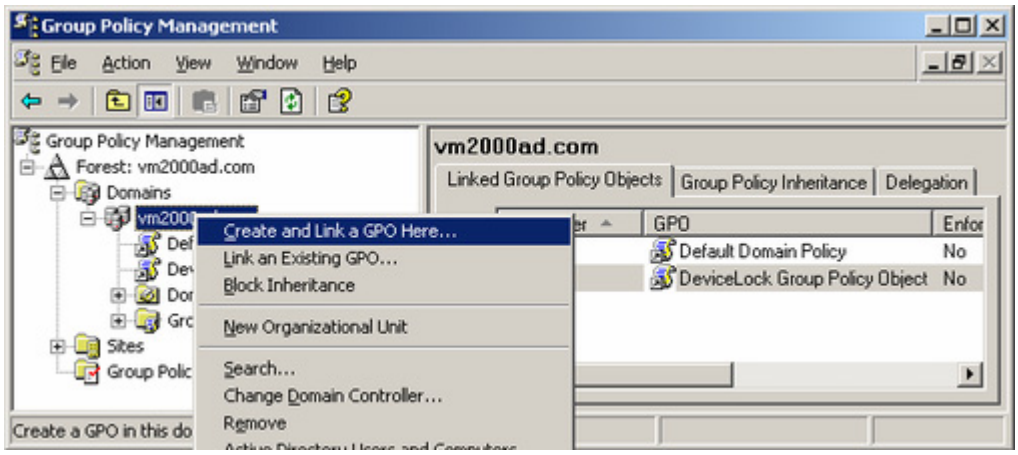
Pour distribuer DeviceLock Service à l'aide de la politique de groupe, procédez comme suit:

- **Créez un point de distribution**
  Pour installer DeviceLock Service, vous devez créer un point de distribution sur le serveur:
  1. Connectez-vous à l'ordinateur serveur en tant qu'administrateur.
  2. Créez un dossier de partage réseau pour y placer le progiciel MSI.
  3. Réglez les autorisations de partage pour permettre l'accès au progiciel de distribution.
  4. Copiez le progiciel MSI (DeviceLock Service.msi et/ou DeviceLock Service x64.msi) dans le point de distribution.

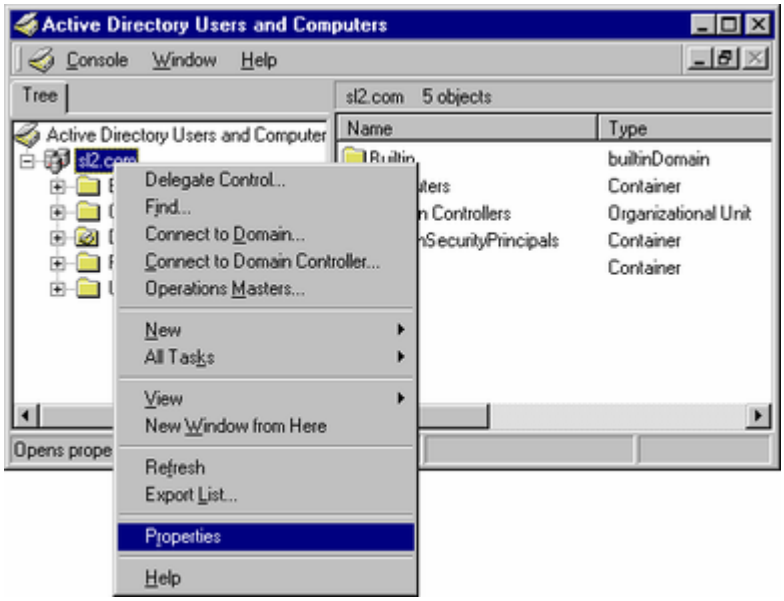
- **Créer une politique de groupe (GPO)**
  Pour créer une politique de groupe (GPO) permettant de distribuer DeviceLock Service:
  1. Démarrez le module Group Policy Management intégré.

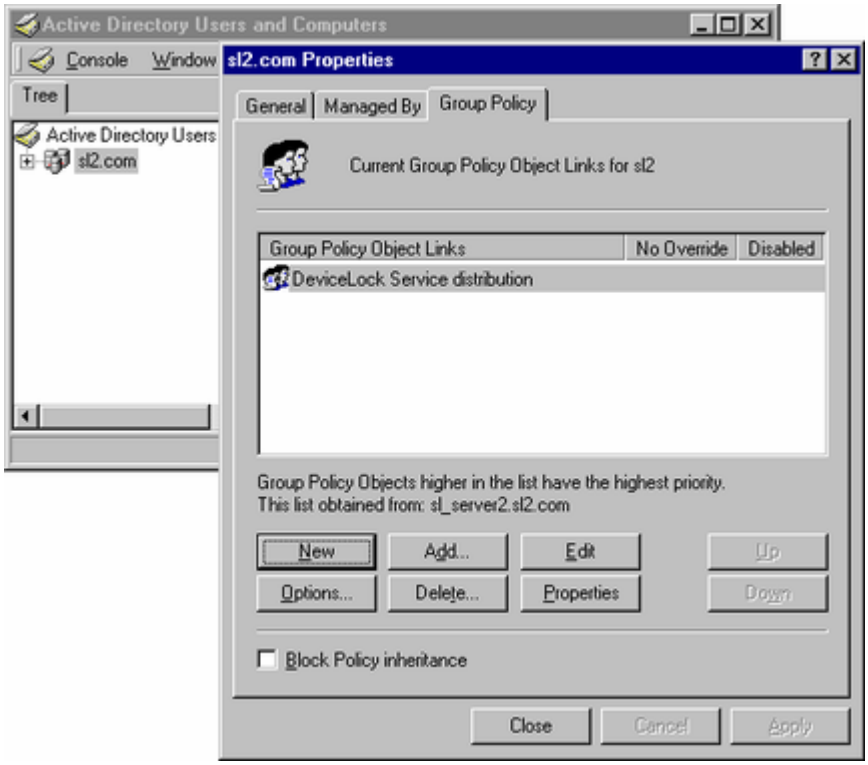
Si le module Group Policy Management n'est pas installé sur votre ordinateur, vous pouvez le remplacer par le module Active Directory Users and Computers.

2. Dans l'arborescence de console, sélectionnez votre domaine.

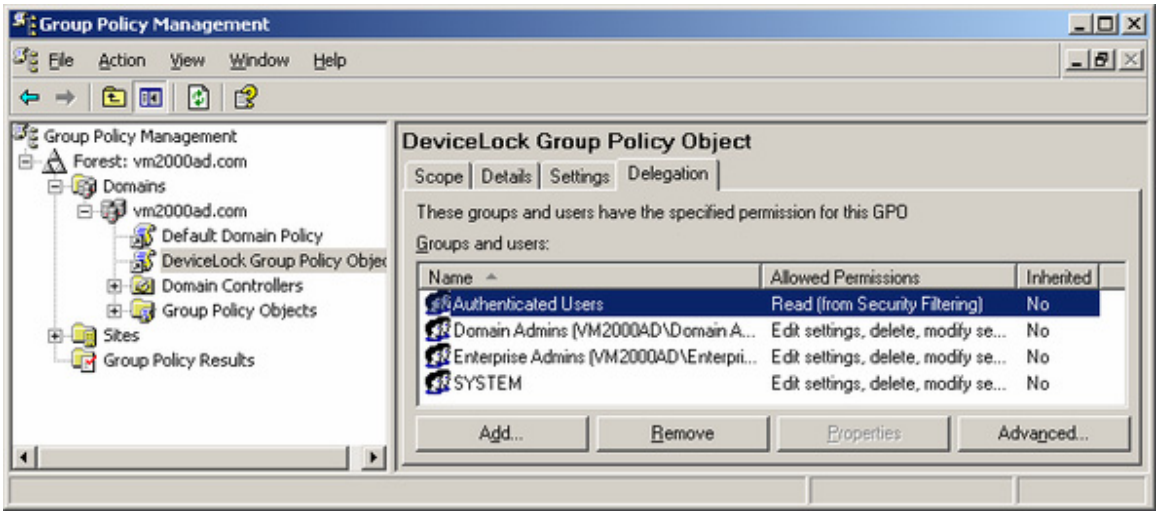


3. Cliquez sur l'option **Create and Link a GPO Here** du menu contextuel de l'élément de domaine. Si vous utilisez le module Active Directory Users and Computers, cliquez droit sur votre domaine, puis cliquez sur **Properties**, sur l'onglet **Group Policy**, et finalement sur **New**.

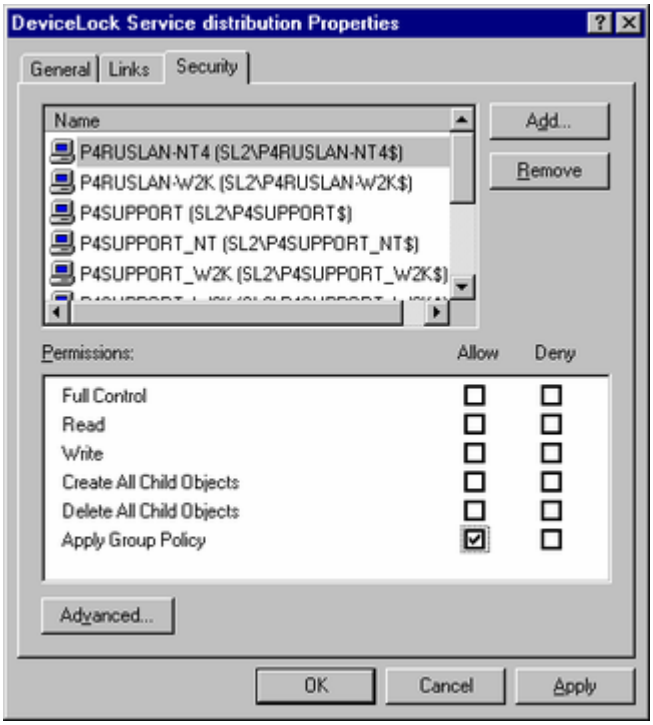




4. Attribuez le nom de votre choix à cette politique, puis appuyez sur ENTREE.
5. Dans l'arborescence de console, sélectionnez votre politique de groupe, cliquez sur l'onglet **Delegation**, puis sur **Advanced**.



- Si vous utilisez le module Active Directory Users and Computers, cliquez sur l'option **Properties** de l'onglet **Group Policy**, puis sur l'onglet **Security**.



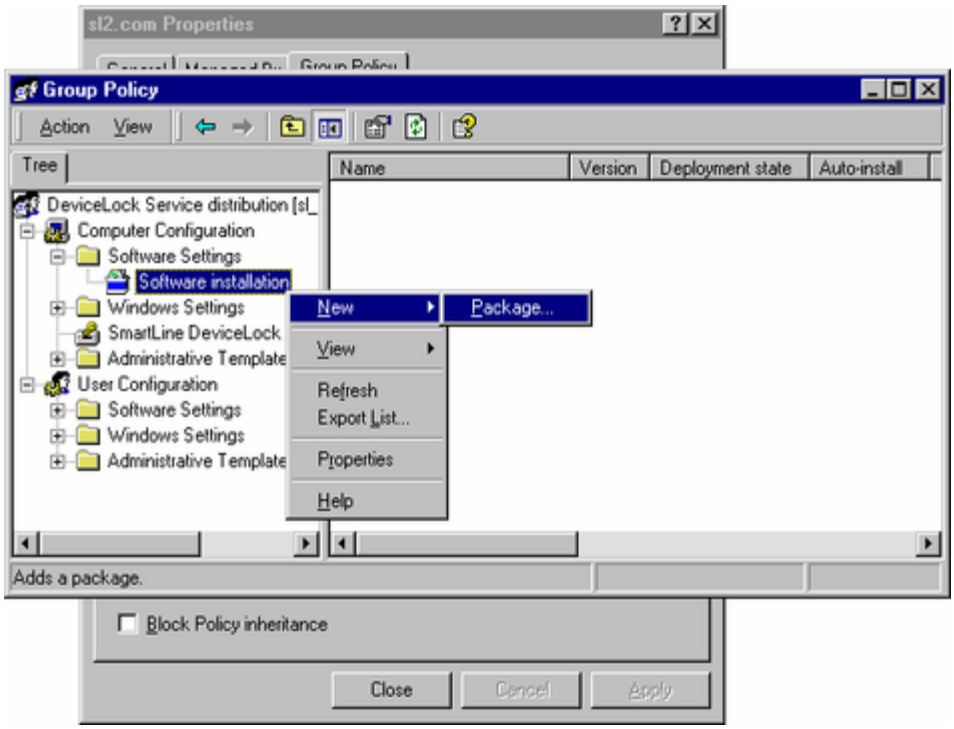
6. Cochez la case **Deny** située à côté d'**Apply Group Policy** pour indiquer les groupes de sécurité auxquels vous ne voulez pas que cette politique s'applique.

   Cochez la case **Allow** pour indiquer les groupes auxquels vous souhaitez que cette politique s'applique. Puis, cliquez sur **OK**.

- **Assigner un progiciel**

  Pour assigner DeviceLock Service aux ordinateurs qui fonctionnent sous Windows 2000 ou une version ultérieure:

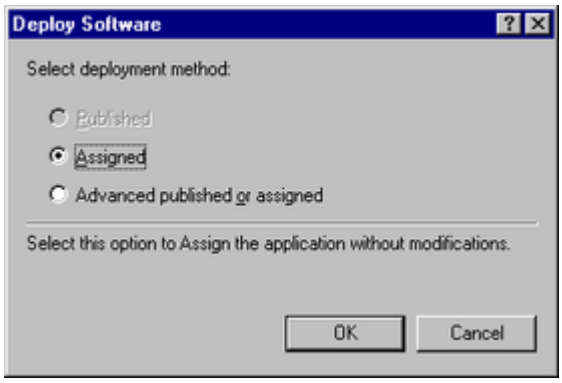
  1. Ouvrez la politique de groupe dont vous avez besoin dans l'éditeur de politique de groupe de Windows (en utilisant soit le module Groupe Policy Management, soit le module Active Directory Users and Computers).
  2. Dans **Computer Configuration**, développez **Software Settings**.
  3. Cliquez droit sur **Software installation**, pointez sur **New** et cliquez sur **Package**.



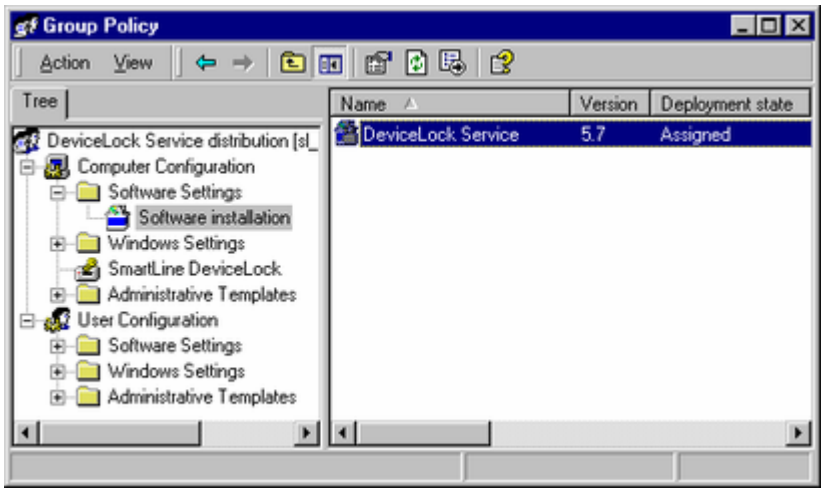
4. Dans la boîte de dialogue **Open**, saisissez le chemin complet de Universal Naming Convention (UNC) menant au dossier partagé qui contient le progiciel MSI de DeviceLock Service. Par exemple : \\file server\share\DeviceLock Service.msi.

IMPORTANT: Ne naviguez pas directement vers l'emplacement, assurez-vous que vous utilisez bien le chemin UNC menant au dossier partagé.

5. Cliquez sur **Open**.
6. Cliquez sur **Assigned**, puis sur **OK**. Le progiciel apparaît dans la liste figurant à droite de la fenêtre **Group Policy**.



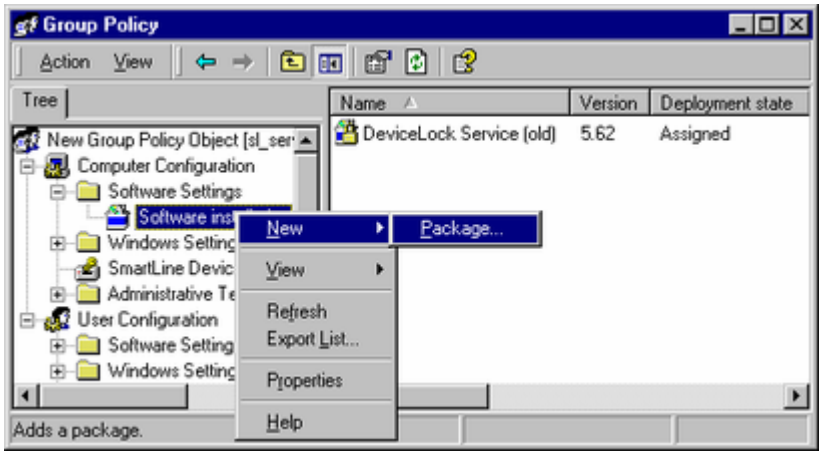
7. Fermez l'éditeur de politique de groupe de Windows. Lors du démarrage de l'ordinateur client, DeviceLock Service s'installera automatiquement.



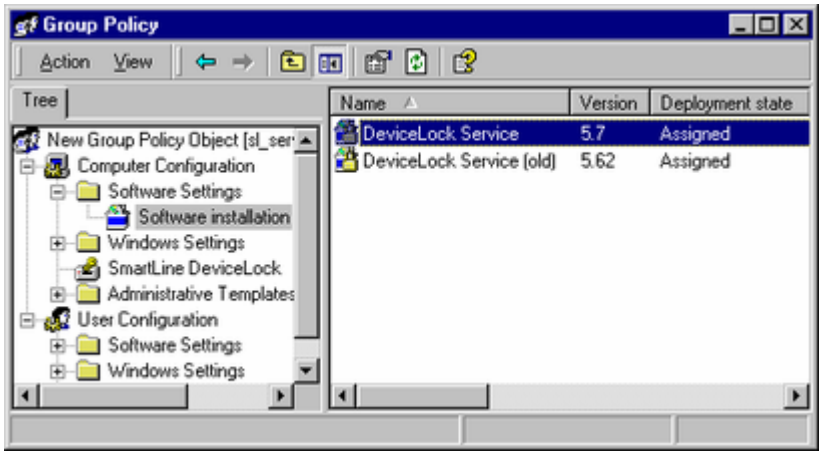
- **Mise à jour de progiciel**

  Si vous avez déjà déployé la version précédente de DeviceLock Service et que vous souhaitez la mettre à jour avec la nouvelle version:

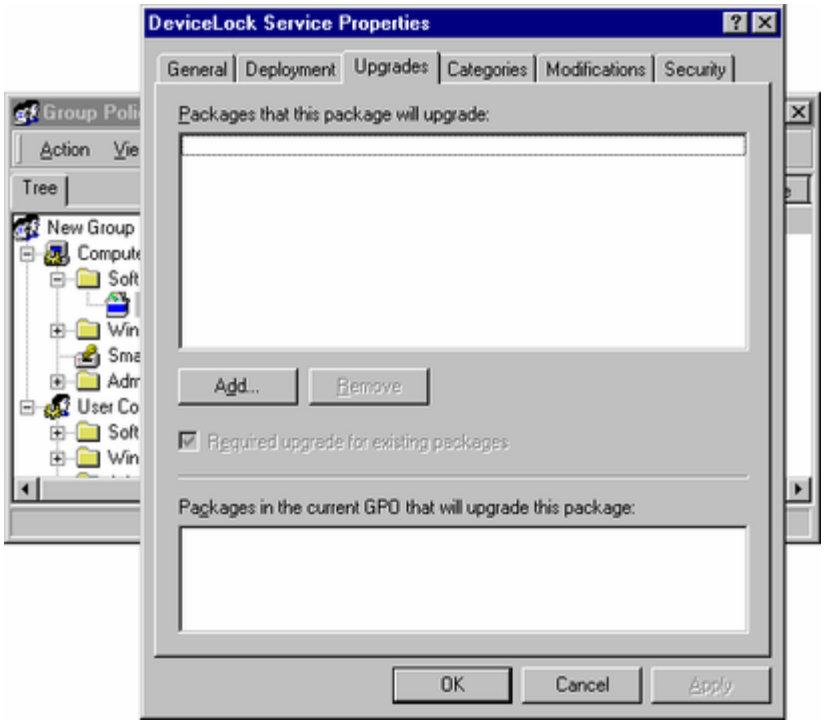
  1. Ouvrez la politique de groupe qui contient l'ancien DeviceLock Service dans l'éditeur de politique de groupe de Windows (en utilisant soit le module Group Policy Management, soit le module Active Directory Users and Computers).
  2. Dans **Computer Configuration**, développez **Software Settings**.
  3. Cliquez droit sur **Software installation**, pointez sur **New** et cliquez sur **Package**.



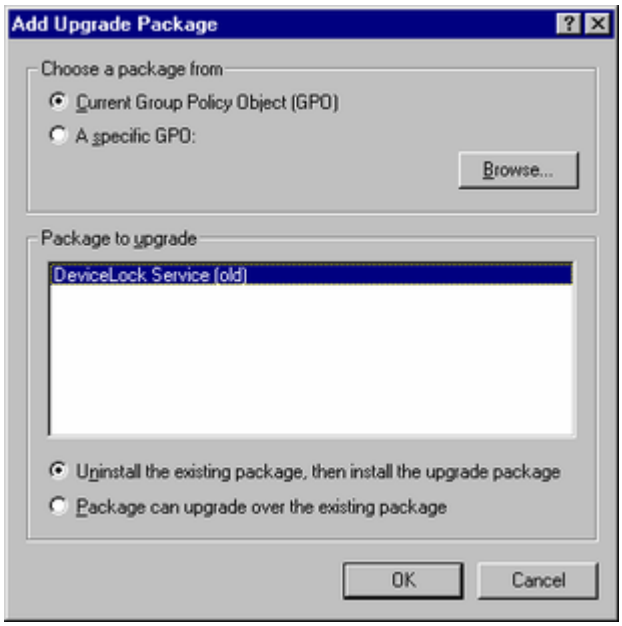
  4. Dans la boîte de dialogue **Open**, tapez le chemin complet de Universal Naming Convention (UNC) menant au dossier partagé qui contient le nouveau progiciel MSI de DeviceLock Service. Par exemple: \\file server\share\DeviceLock Service.msi.
  5. Cliquez sur **Open**.
  6. Cliquez sur **Assigned**, puis sur **OK**. Le nouveau progiciel apparaît dans la liste figurant à droite de la fenêtre **Group Policy**.



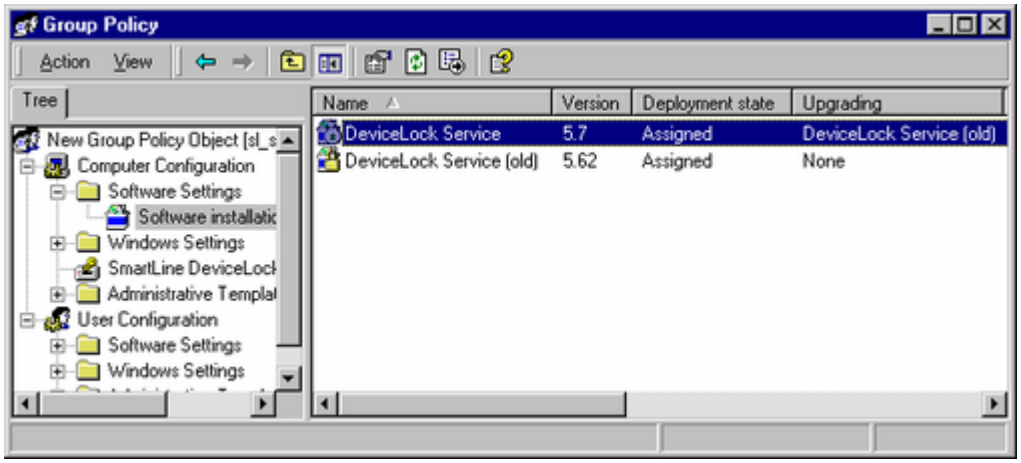
7. Faites un clic droit sur le nouveau progiciel, cliquez sur **Properties**, puis sur l'onglet **Upgrades**.



8. Cliquez sur **Add**, et choisissez l'ancien DeviceLock Service que vous souhaitez mettre à jour, cliquez sur **Uninstall the existing package, then install the upgrade package**, puis sur **OK**.



9. Cliquez sur **OK** pour fermer la fenêtre **Properties**, et fermez l'éditeur de politique de groupe de Windows. Au démarrage de l'ordinateur client, DeviceLock Service sera automatiquement mis à jour.



Remarque: En principe, lorsque vous effectuez des mises à jour, le nouveau progiciel MSI DeviceLock Service détecte le progiciel assigné précédemment dans le GPO et accomplit les étapes 7 et 8 ci-dessus automatiquement.

- **Redéployer un progiciel**

  Vous risquez parfois de devoir redéployer DeviceLock Service.

  Dans ce cas,

  1. Ouvrez la politique de groupe qui contient le progiciel déployé dans l'éditeur de politique de groupe de Windows (en utilisant soit le module Group Policy Management, soit le module Active Directory Users and Computers).

2. Ouvrez le dossier **Software Settings** qui contient l'élément **Software installation** avec lequel vous avez installé le progiciel.
3. Cliquez sur le dossier **Software installation** qui contient le progiciel.
4. Dans le panneau de droite de la fenêtre **Group Policy**, cliquez droit sur le programme, pointez la souris sur **All Tasks**, puis cliquez sur **Redeploy applicatio**n. Le message suivant s'affiche: "**Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?**"
5. Cliquez sur **Yes**.
6. Fermez l'éditeur de politique de groupe de Windows.

- **Supprimer un progiciel**

  Pour supprimer DeviceLock Service:

  1. Ouvrez la politique de groupe qui contient le progiciel déployé dans l'éditeur de politique de groupe de Windows (en utilisant soit le module Group Policy Management, soit le module Active Directory Users and Computers).
  2. Ouvrez le dossier **Software Settings** qui contient l'élément **Software installation** avec lequel vous avez installé le progiciel.
  3. Cliquez sur le dossier **Software installation** qui contient le progiciel.
  4. Dans le panneau de droite de la fenêtre **Group Policy**, cliquez droit sur le programme. Pointez la souris sur **All Tasks**, puis cliquez sur **Remove**.
  5. Cliquez sur **Immediately uninstall the software from users and computers**, puis sur **OK**.
  6. Fermez l'éditeur de politique de groupe de Windows.

Gardez à l'esprit les points suivants:

- Le déploiement de l'application se produit uniquement et une fois pour toute au démarrage de l'ordinateur, et non de façon périodique. Ceci évite des phénomènes indésirables tels que la désinstallation ou la mise à jour intempestive d'une application en cours d'utilisation.
- DeviceLock Service sera copié dans le répertoire %ProgramFiles%\DeviceLock Agent si ce service n'existe pas déjà sur le système. Si le service existe déjà sur ce système, mais dans une version antérieure à la version 7.0, DeviceLock Service sera également copié dans le répertoire par défaut %ProgramFiles%\DeviceLock Agent. Si la version 7.0 (ou une version supérieure) de ce service existe sur le système, DeviceLock Service sera copié dans le répertoire de l'ancienne version, et celle-ci sera automatiquement remplacée.

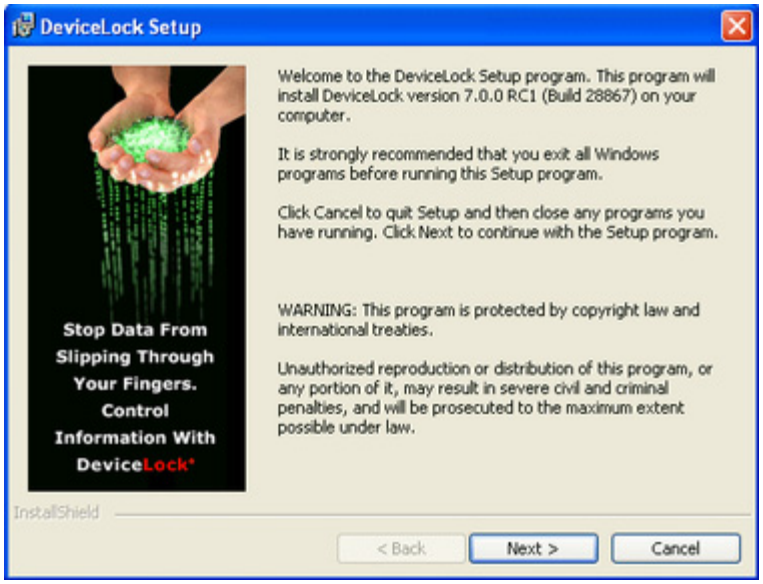
Installation des consoles de gestion

Les consoles de gestion DeviceLock sont les interfaces de contrôle qu'utilisent les administrateurs systèmes pour paramétrer à distance DeviceLock Service, DeviceLock Enterprise Server et DeviceLock Content Security Server.

Les consoles de gestion de DeviceLock doivent être installées sur l'ordinateur à partir duquel l'administrateur gérera la configuration de DeviceLock et créera des rapports. Inutile d'installer des consoles de gestion sur le serveur (contrôleur de domaine ou autres), même si vous envisagez d'utiliser DeviceLock Group Policy Manager pour administrer les configurations via Active Directory Group Policy: vous pouvez le faire à partir de votre poste de travail local (en fonction des privilèges accordés).

Remarque: Pour pouvoir utiliser DeviceLock Management Console (le module MMC) et DeviceLock Service Settings Editor sur des ordinateurs sous Windows NT 4.0, il faut installer la mise à jour de Microsoft Management Console. Cette mise à jour peut être téléchargée gratuitement à partir du site Web de Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=3F620A07-C996-4A81-AAD8-30134A43EC46&displaylang=en.

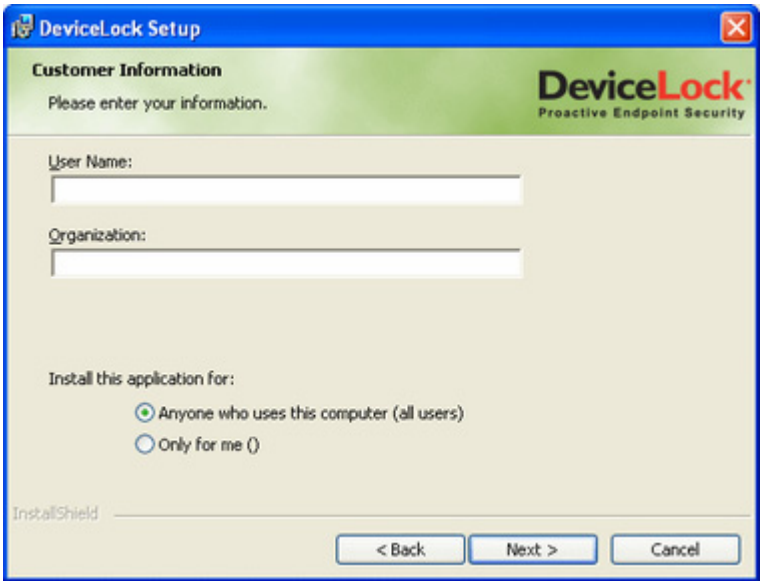
Exécutez le programme de configuration (**setup.exe**) et suivez les instructions qui apparaissent à l'écran.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

Vous devez accepter le contrat de licence d'utilisateur final de DeviceLock avant de continuer la procédure d'installation.

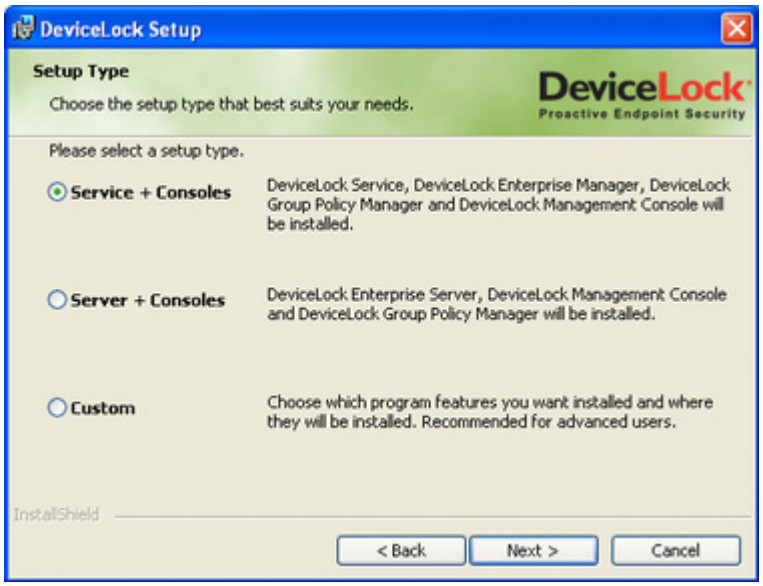
Dans la page **Customer Information** (informations du client), saisissez votre nom d'utilisateur et celui de votre organisation. Dans cette même page, sous **Install this application for** (installer cette application pour), vous pouvez indiquer les utilisateurs pour lesquels des raccourcis bureau vers les consoles de gestion DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager et DeviceLock Service Settings Editor) seront créés. Vous pouvez sélectionner l'une ou l'autre des options suivantes:

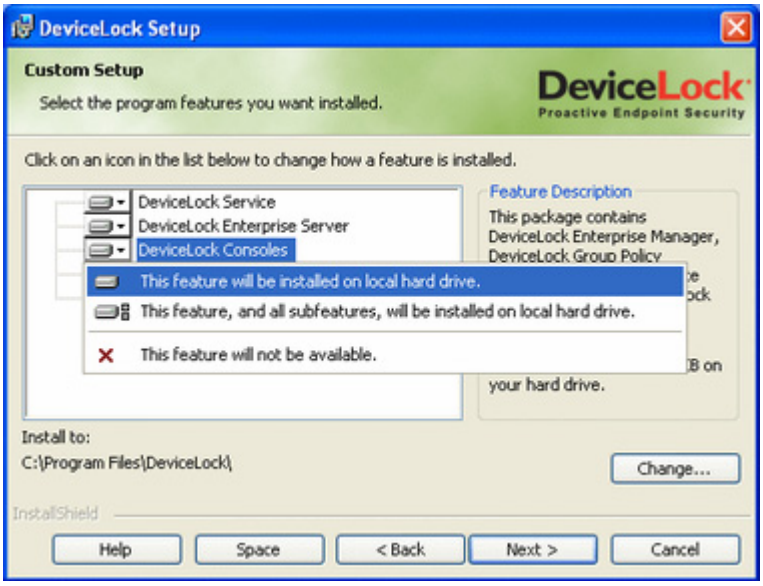
- **Anyone who uses this computer (all users)** (tous les utilisateurs): crée des raccourcis bureau vers les consoles de gestion DeviceLock pour tous les utilisateurs.
- **Only for me** (pour moi uniquement): crée des raccourcis bureau vers les consoles de gestion DeviceLock uniquement pour le compte d'utilisateur effectuant l'installation de DeviceLock.



Dans la page **Setup type** (type de configuration), sélectionnez le type de configuration requis.

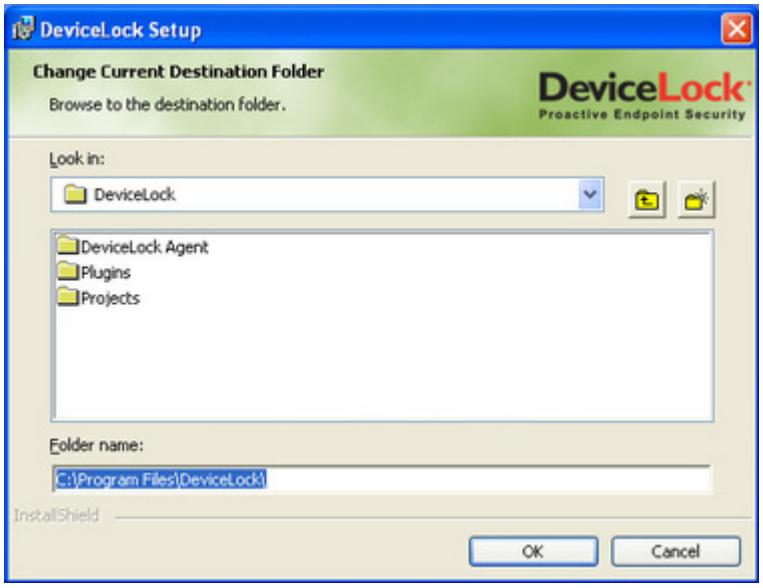
Vous pouvez, au choix: opter pour l'installation conjuguée de DeviceLock Service et des consoles de gestion de DeviceLock en utilisant la configuration **Services + Consoles**, installer DeviceLock Enterprise Server et les consoles de gestion en utilisant la configuration **Server + Consoles** ou n'installer que les consoles de gestion en utilisant la configuration personnalisée (cochez **Custom** et sélectionnez la composante **DeviceLock Consoles**).


DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel


DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
DeviceLock Enterprise Server
DeviceLock Consoles
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
Feature Description
This package contains DeviceLock Enterprise Manager, DeviceLock Group Policy
your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

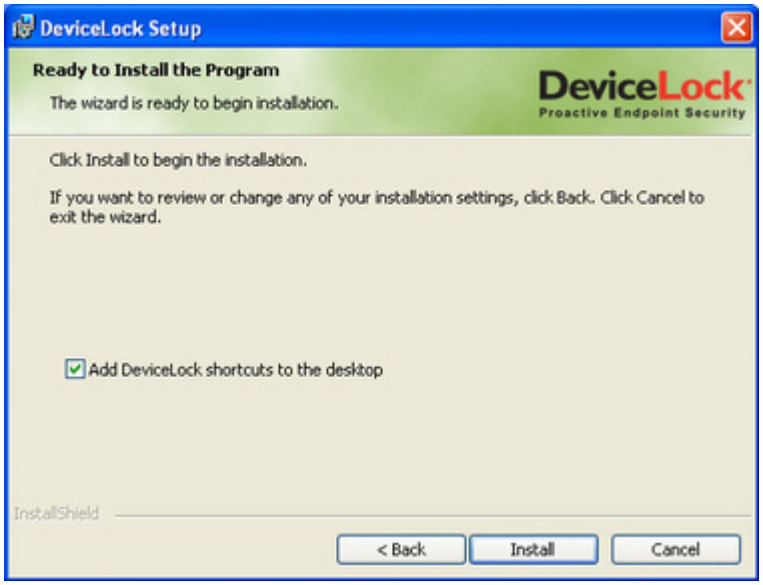
Remarque: Dans la page **Custom Setup** (configuration personnalisée), choisissez le composant RSoP à installer. Ce composant active l'assistance pour le mode de planification de DeviceLock's Resultant Set of Policy sur les contrôleurs de domaine. Le composant RSoP n'est nécessaire que lorsque les consoles de gestion DeviceLock sont installées sur l'ordinateur, mais pas DeviceLock Service. Pour plus d'informations sur le mode de planification RSoP, visitez la page Microsoft documentation.

Dans la page **Custom Setup**, vous pouvez changer le répertoire d'installation par défaut. Le répertoire d'installation par défaut de DeviceLock est **%ProgramFiles%\DeviceLock**. Pour changer le répertoire d'installation, cliquez sur **Change** pour accéder à la page **Change Current Destination Folder** (répertoire d'installation actuel) et effectuer les modifications nécessaires.



DeviceLock est livré avec trois consoles de gestion différentes: DeviceLock Management Console (l'extension MMC), DeviceLock Enterprise Manager et DeviceLock Group Policy Manager (intégré dans l'éditeur de politique de groupe de Windows). DeviceLock Service Settings Editor, installé en même temps que les autres consoles de gestion, est un outil qui permet de créer et de modifier les fichiers XML externes avec les paramètres, les autorisations, les règles d'audit et de réplication de DeviceLock Service.

Dans la page **Ready to Install the Program** (prêt pour l'installation), cliquez sur **Install** pour démarrer l'installation. Cochez la case **Add DeviceLock shortcuts to the desktop** si vous désirez créer des raccourcis vers DeviceLock Management Console (le module MMC), DeviceLock Enterprise Manager et DeviceLock Service Settings Editor sur le bureau.

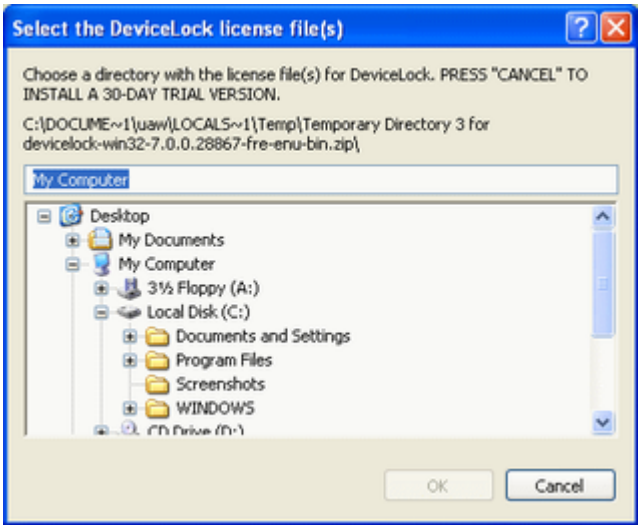

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Le programme de configuration pourra vous proposer de créer un nouveau DeviceLock Certificate.

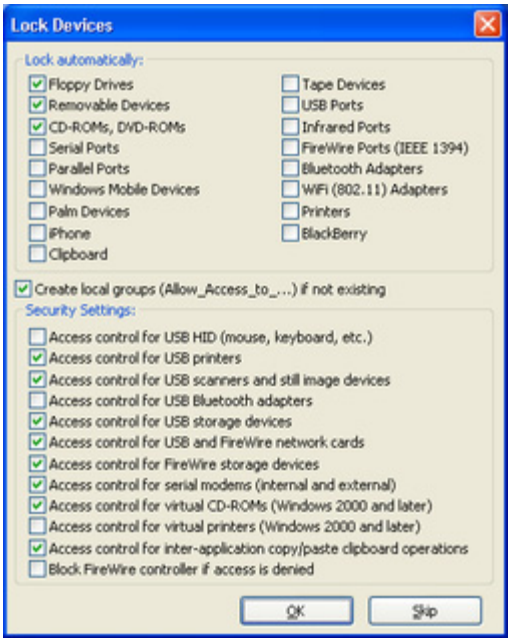
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

Vous pourrez toujours créer le nouveau certificat plus tard, en utilisant l'outil de création de certificat installé avec les consoles de gestion DeviceLock. Par conséquent, si à ce stade vous ne savez pas si vous avez besoin du nouveau certificat, il vous suffit de cliquer sur **No** pour continuer l'installation. Pour des informations détaillées sur les DeviceLock Certificates, consultez le chapitre «DeviceLock Certificates.»

L'assistant d'installation pourra aussi vous proposer de charger les fichiers de licence DeviceLock. Si vous n'avez pas de fichier de licence, cliquez sur le bouton **Cancel** pour installer DeviceLock en mode essai de trente jours.

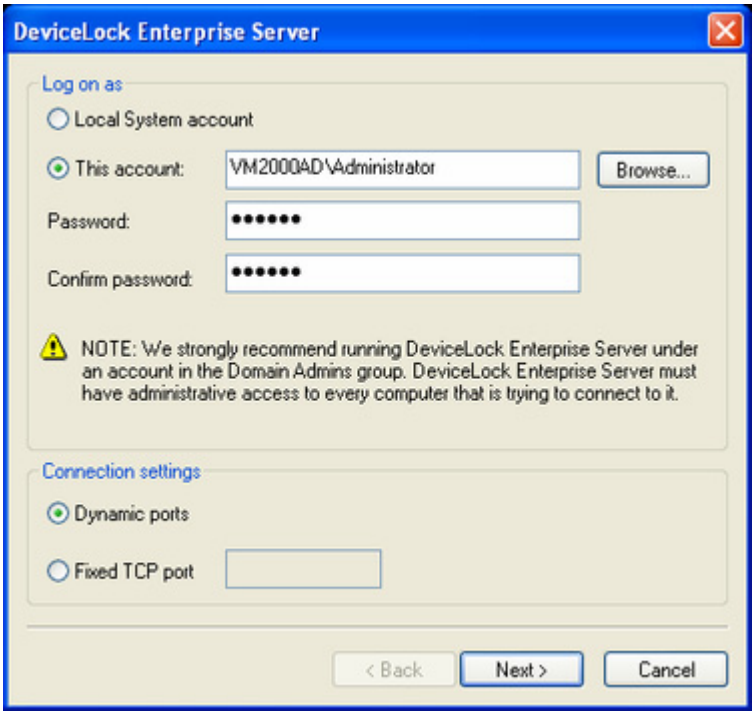


Si vous avez aussi choisi d'installer DeviceLock Service, le programme de configuration vous suggère de définir les autorisations pour les périphériques locaux.



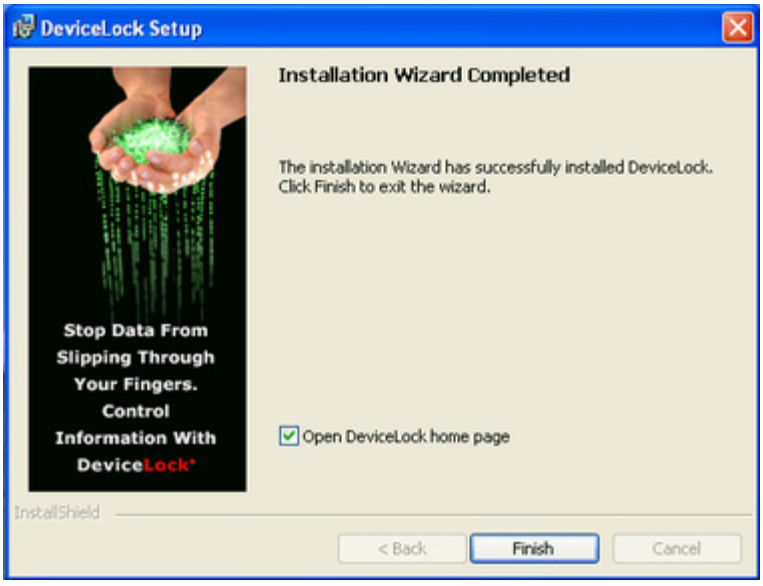
Cliquez sur **Skip** si vous préférez attendre la fin de l'installation pour configurer les autorisations d'accès aux périphériques en utilisant les consoles de gestion de DeviceLock.

Pour plus de détails sur ces options, veuillez vous reporter au chapitre Déploiement de DeviceLock Service de ce manuel. Si vous avez aussi choisi d'installer DeviceLock Enterprise Server, le programme de configuration vous suggère d'en définir les paramètres à l'aide de l'assistant de configuration.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

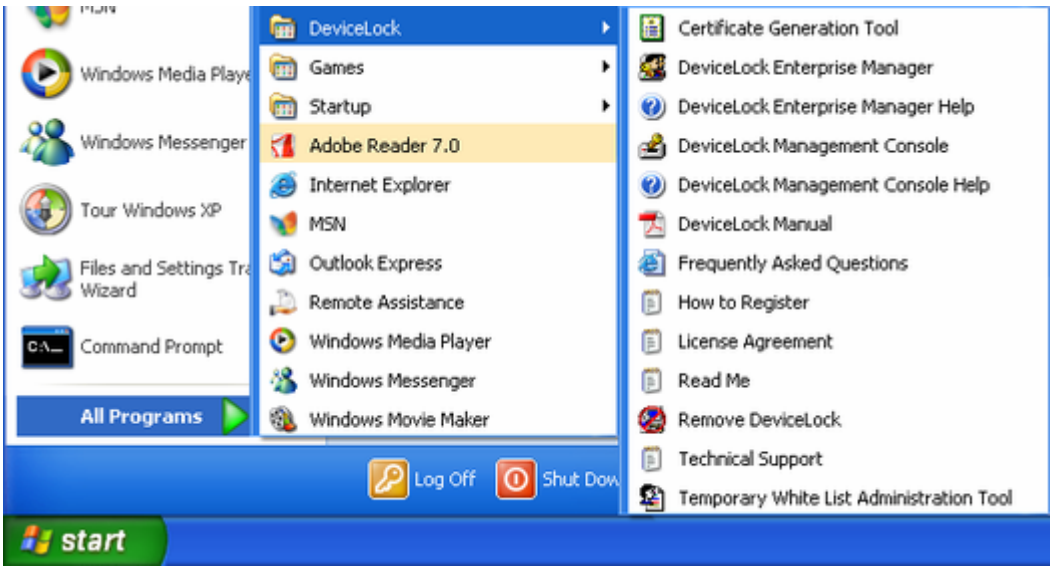
Pour en savoir plus sur ces options, veuillez vous reporter au chapitre Installation de DeviceLock Enterprise Server de ce manuel.

Dès que le programme de configuration a terminé l'installation de DeviceLock, il vous propose de visiter le site Web de DeviceLock.


DeviceLock Setup
Installation Wizard Completed
The installation Wizard has successfully installed DeviceLock. Click Finish to exit the wizard.
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Open DeviceLock home page
InstallShield
< Back
Finish
Cancel

Décochez la case **Open DeviceLock home page** si vous ne désirez pas visiter le site Web de DeviceLock. Cliquez sur le bouton **Finish** pour terminer l'installation.

Vous pouvez retrouver et lancer les consoles de gestion DeviceLock à l'aide du menu **All Programs**, disponible via le bouton **Start** de Windows.



Remarque: DeviceLock Group Policy Manager fait partie de l'éditeur de politique de groupe de Windows et n'est pas disponible en tant que logiciel autonome. Pour pouvoir utiliser DeviceLock Group Policy Manager, vous devez utiliser l'éditeur de politique de groupe standard de Windows.

Pour désinstaller DeviceLock, effectuer l'une ou l'autre des actions suivantes:

Utilisez l'option **Ajouter ou supprimer des programmes** du panneau de commande pour supprimer **DeviceLock**.
- OU -
Cliquez sur **Démarrer**, sélectionnez **Tous les programmes**, puis **DeviceLock**, et cliquez sur **Remove DeviceLock**.

Installation de DeviceLock Enterprise Server

DeviceLock Enterprise Server est l'élément optionnel de collecte et de stockage centralisé des données de réplication et des registres d'audit. DeviceLock Enterprise Server peut aussi surveiller les ordinateurs distants en temps réel, en vérifiant le statut de DeviceLock Service (actif ou non), ainsi que la consistance et l'intégrité de la politique utilisée.

Pour utiliser DeviceLock Enterprise Server avec des ordinateurs sous Windows NT4.0 SP6 et Windows 2000, il faut installer Microsoft Data Access Components (MDAC), version 2.8 ou supérieure. MDAC est disponible en téléchargement gratuit à partir du site Web de Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&displaylang=fr.

Planification de l'infrastructure

Vous pouvez installer plusieurs DeviceLock Enterprise Servers sur différents ordinateurs afin de répartir uniformément la charge du réseau.

DeviceLock Enterprise Server utilise MS SQL Server pour stocker les données. Par conséquent, MS SQL Server doit être installé et activé sur le réseau avant d'installer DeviceLock Enterprise Server. Si vous ne disposez pas de MS SQL Server, vous pouvez installer la version gratuite, SQL Server Express Edition, téléchargeable à partir du site Web de Microsoft: http://msdn.microsoft.com/vstudio/express/sql/download/.

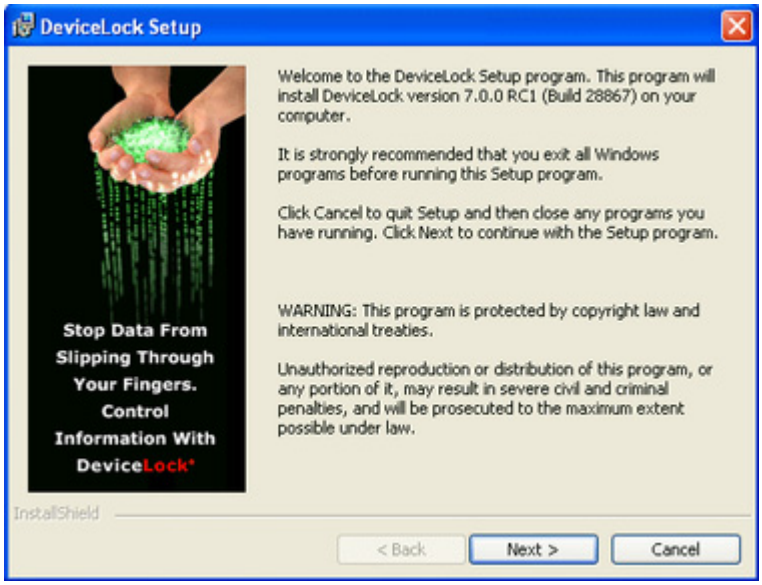
MS SQL Server et DeviceLock Enterprise Server ne doivent pas obligatoirement fonctionner sur la même machine; de fait, pour améliorer les performances et la stabilité, il est préférable d'installer DeviceLock Enterprise Server sur un ordinateur indépendant.

Pour la connexion entre DeviceLock Enterprise Server et MS SQL Server, trois cas de figure peuvent se présenter. A vous de décider lequel est le plus adapté à vos besoins, avant d'installer DeviceLock Enterprise Server.

1. ONE-TO-ONE: Vous installez un DeviceLock Enterprise Server, et le connectez à un MS SQL Server. Ce cas de figure est le plus adapté aux petits réseaux (jusqu'à quelques centaines d'ordinateurs).
2. MANY-TO-MANY: Vous installez plusieurs DeviceLock Enterprise Servers ; chacun est connecté à son propre MS SQL Server. Ce cas de figure correspond typiquement aux moyens et grands réseaux géographiquement étendus sur une variété de secteurs.
3. MANY-TO-ONE: Vous installez plusieurs DeviceLock Enterprise Servers, tous connectés à un seul MS SQL Server. Ce cas de figure peut convenir à un réseau moyen ou grand avec une machine puissante (tant en mémoire vive qu'en espace de stockage libre), dédiée à MS SQL Server.

Installation interactive

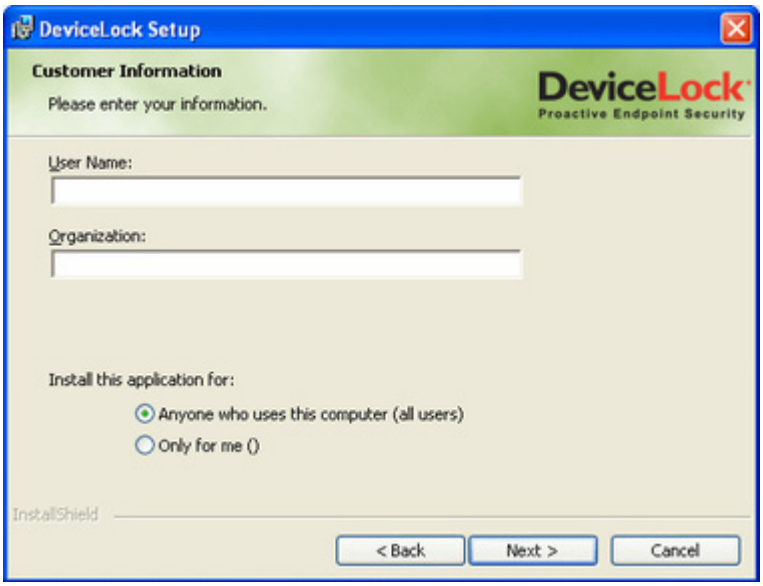
Exécutez le programme de configuration (**setup.exe**) et suivez les instructions qui apparaissent à l'écran. Vous devez exécuter **setup.exe** sur chacun des ordinateurs sur lesquels vous voulez installer DeviceLock Enterprise Server.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

Vous devez accepter le contrat de licence d'utilisateur final de DeviceLock avant de continuer la procédure d'installation.

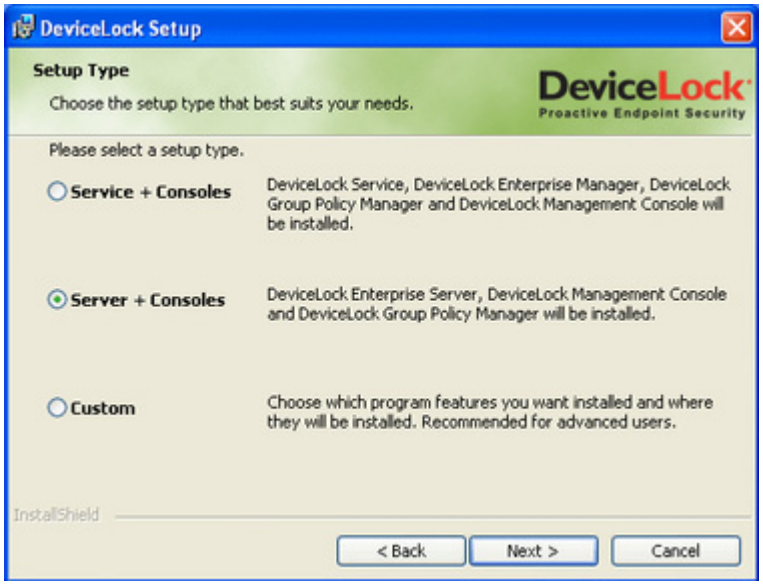
Dans la page **Customer Information** (informations du client), saisissez votre nom d'utilisateur et celui de votre organisation. Dans cette même page, sous **Install this application for** (installer cette application pour), vous pouvez indiquer les utilisateurs pour lesquels des raccourcis bureau vers les consoles de gestion DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager et DeviceLock Service Settings Editor) seront créés. Vous pouvez sélectionner l'une ou l'autre des options suivantes:

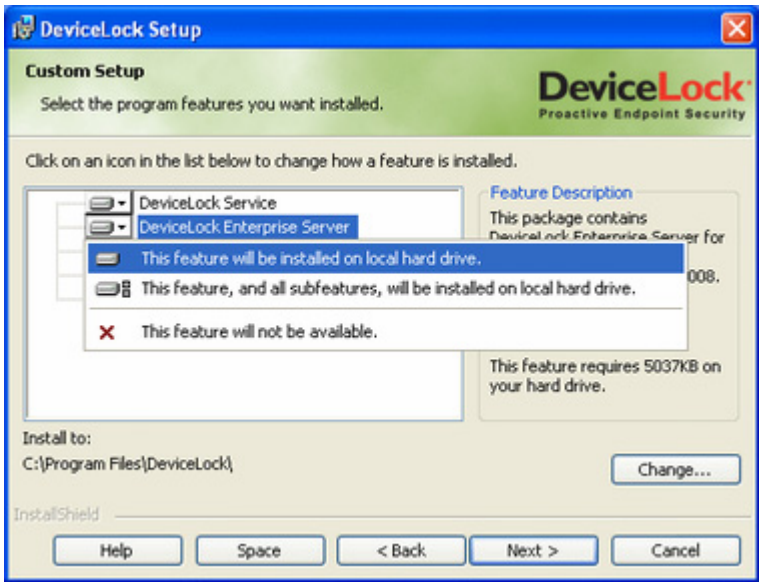
- **Anyone who uses this computer (all users)** (tous les utilisateurs): crée des raccourcis bureau vers les consoles de gestion DeviceLock pour tous les utilisateurs.
- **Only for me** (pour moi uniquement): crée des raccourcis bureau vers les consoles de gestion DeviceLock uniquement pour le compte d'utilisateur effectuant l'installation de DeviceLock.



Dans la page **Setup type** (type de configuration), sélectionnez le type de configuration requis.

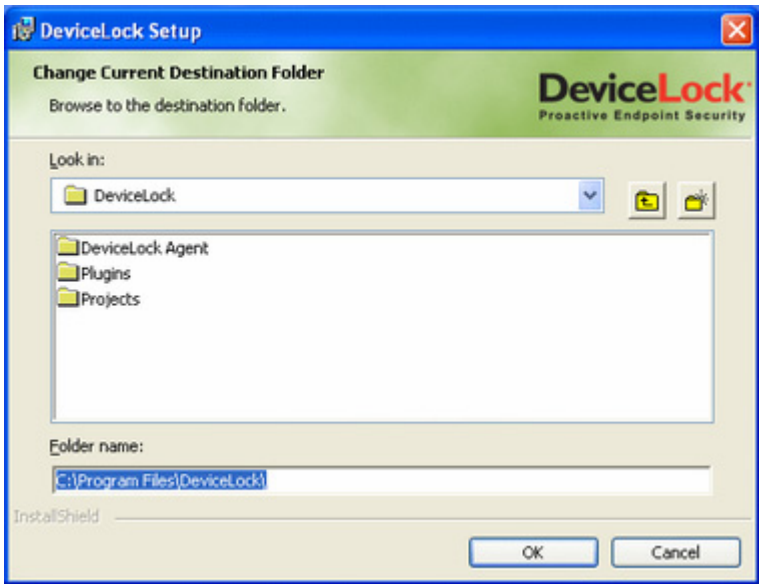
Vous pouvez, au choix: opter pour l'installation conjuguée de DeviceLock Enterprise Server et des consoles de gestion de DeviceLock à l'aide de l'option **Server + Consoles** ou choisir d'installer seulement DeviceLock Enterprise Server à l'aide de la configuration personnalisée (cochez **Custom** et sélectionnez le composant **DeviceLock Enterprise Server**).


DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

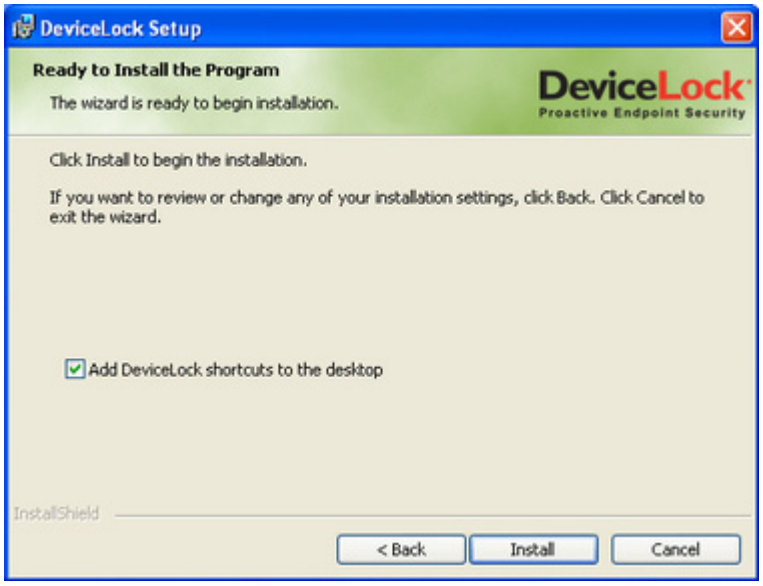

DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
DeviceLock Enterprise Server
Feature Description
This package contains
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
This feature requires 5037KB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Remarque: Dans la page **Custom Setup** (configuration personnalisée), choisissez le composant RSoP à installer. Ce composant active l'assistance pour le mode de planification de DeviceLock's Resultant Set of Policy sur les contrôleurs de domaine. Le composant RSoP n'est nécessaire que lorsque les consoles de gestion DeviceLock sont installées sur l'ordinateur, mais pas DeviceLock Service. Pour plus d'informations sur le mode de planification RSoP, visitez la page Microsoft documentation.

Dans la page **Custom Setup**, vous pouvez changer le répertoire d'installation par défaut. Le répertoire d'installation par défaut de DeviceLock est **%ProgramFiles%\DeviceLock**. Pour changer le répertoire d'installation, cliquez sur **Change** pour accéder à la page **Change Current Destination Folder** (répertoire d'installation actuel) et effectuer les modifications nécessaires.



Dans la page **Ready to Install the Program** (prêt pour l'installation), cliquez sur **Install** pour démarrer l'installation. Cochez la case **Add DeviceLock shortcuts to the desktop** si vous désirez créer des raccourcis vers DeviceLock Management Console (le module MMC), DeviceLock Enterprise Manager et DeviceLock Service Settings Editor sur le bureau.

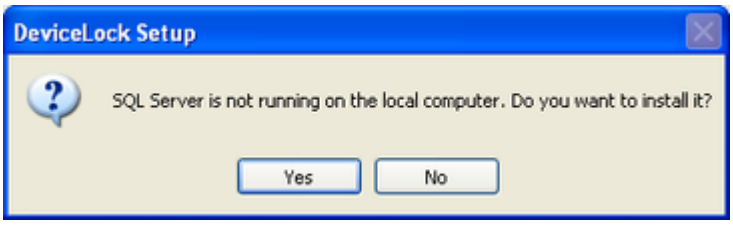

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Si vous avez choisi d'installer aussi les consoles de gestion DeviceLock, le programme de configuration risque de vous proposer de créer un nouveau DeviceLock Certificate.

DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

Vous pourrez toujours créer le nouveau certificat plus tard, en utilisant l'outil de création de certificat installé avec les consoles de gestion DeviceLock. Par conséquent, si à ce stade vous ne savez pas si vous avez besoin du nouveau certificat, il vous suffit de cliquer sur **No** pour continuer l'installation. Pour des informations détaillées sur les DeviceLock Certificates, consultez le chapitre «DeviceLock Certificates.»

Si le programme de configuration détecte que MS SQL Server n'est pas présent sur l'ordinateur local, mais que le programme d'installation est disponible, le programme de configuration vous propose de démarrer l'installation de MS SQL Server.



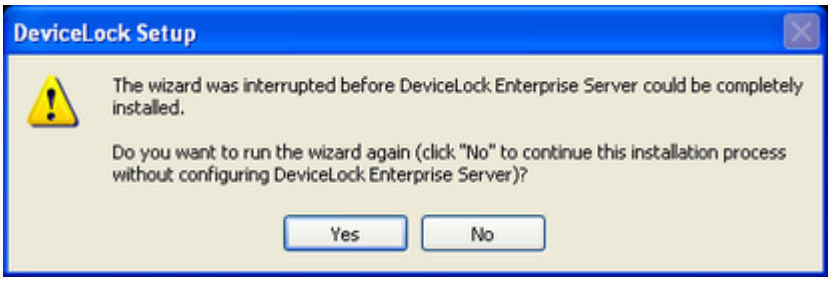
Si vous ne souhaitez pas installer MAS SQL Server sur l'ordinateur local, ou si MS SQL Server est installé mais n'a pas été activé, cliquez sur **No**.

Lors du processus d'installation, vous devez configurer DeviceLock Enterprise Server et définir les paramètres principaux en utilisant l'assistant dédié.

Si vous effectuez une mise à jour ou une réinstallation de DeviceLock Enterprise Server, et souhaitez conserver le paramétrage actuel, inutile de reprendre cet assistant: cliquez sur **Cancel** pour fermer l'assistant et conserver en l'état les paramètres préexistants.

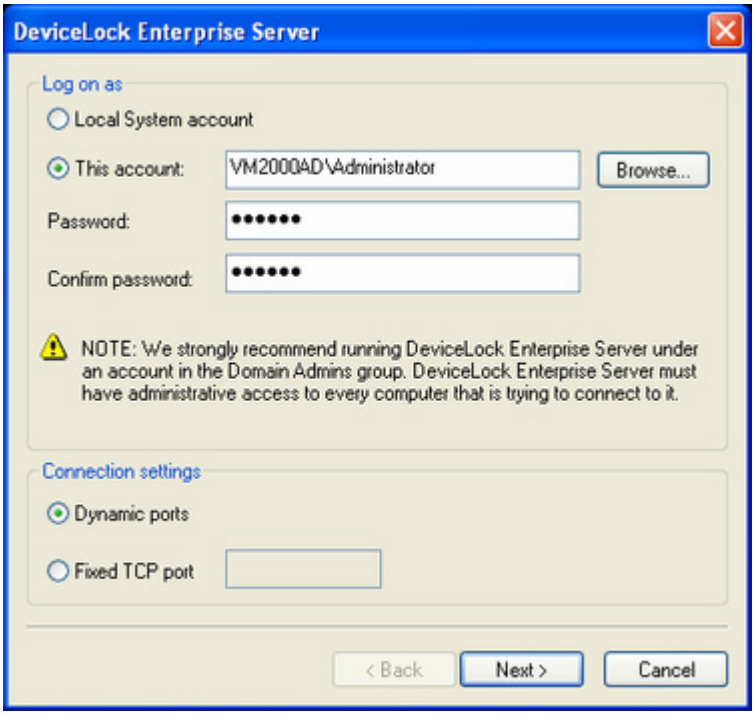
Dans le cas où il vous faudrait changer certains paramètres mais en garder d'autres, éditez les paramètres nécessaires et faites défiler tous les écrans de l'assistant jusqu'au bouton **Finish** de la toute dernière page.

Remarque: Si vous installez DeviceLock Enterprise Server pour la première fois (il n'y a pas encore de paramètres sur cet ordinateur) et que vous annulez l'assistant de configuration au démarrage, l'installateur ne pourra pas installer DeviceLock Enterprise Server; il vous faudra donc relancer l'assistant de configuration.


DeviceLock Setup
The wizard was interrupted before DeviceLock Enterprise Server could be completely installed.
Do you want to run the wizard again (click "No" to continue this installation process without configuring DeviceLock Enterprise Server)?
Yes
No

Si vous appuyez sur **No** pour continuer sans installer DeviceLock Enterprise Server, vous devrez de toute façon exécuter le programme de configuration ultérieurement pour installer le service.

Sur la première page de l'assistant, vous pouvez décider d'installer DeviceLock Enterprise Server et définir les paramètres de démarrage.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

Log on as (se connecter en tant que)
Commencez par choisir un compte de démarrage de DeviceLock Enterprise Server. Comme bien d'autres services Windows, DeviceLock Enterprise Server peut démarrer sous le compte particulier du système local (l'utilisateur SYSTEM), quel que soit l'utilisateur considéré.

Pour démarrer le service avec le compte de l'utilisateur SYSTEM, choisissez l'option **Local System account**. Notez que le processus qui travaille avec le compte SYSTEM ne peut pas accéder aux ressources de réseau partagées, et s'identifie auprès des ordinateurs distants comme un utilisateur anonyme. Par conséquent, DeviceLock Enterprise Server configuré pour fonctionner avec le compte de l'utilisateur SYSTEM ne peut pas stocker des fichiers de réplication sur l'ordinateur distant (par exemple sur le serveur de fichiers), et il devra utiliser DeviceLock Certificate pour l'identification auprès des DeviceLock Services installés sur des ordinateurs distants.

Pour plus d'informations sur les méthodes d'identification, veuillez vous reporter à la description du paramètre Certificate Name.

Pour démarrer le service au nom de l'utilisateur, choisissez l'option **This account**, puis saisissez le nom du compte et le mot de passe. Il est conseillé d'utiliser un compte d'utilisateur qui dispose des privilèges d'administration sur tous les ordinateurs qui exécutent DeviceLock Service. Dans le cas contraire, il vous faudra utiliser l'identification DeviceLock Certificate.

Si vous installez DeviceLock Enterprise Server dans l'environnement de domaine, nous vous conseillons d'utiliser le compte d'un utilisateur qui est membre du groupe Domain Admins. Etant donné que Domain Admins est membre du groupe local

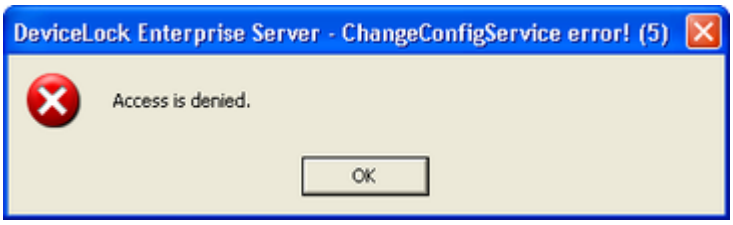
Administrators sur chacun des ordinateurs du domaine, tous les membres de Domain Admins bénéficieront d'un accès libre à DeviceLock Service sur chacun des ordinateurs.

Et n'oubliez pas que si DeviceLock Security est activé sur les DeviceLock Service distants afin de les protéger contre les utilisateurs locaux possédant des droits d'administrateurs, le compte de l'utilisateur mentionné dans le paramètre **This account** doit aussi figurer dans la liste des DeviceLock Administrators bénéficiant de droits **Full access**. Dans le cas contraire, il vous faudra utiliser l'identification DeviceLock Certificate.

Connection settings (Paramètres de connexion)
Vous pouvez ordonner à DeviceLock Enterprise Server d'utiliser un port TCP fixe pour la communication avec la console d'administration, ce qui simplifie la configuration d'un pare-feu, en tapant le numéro de port dans **Fixed TCP port**. Pour utiliser les ports dynamiques pour la communication RPC, cliquez sur **Dynamic ports**. Par défaut, DeviceLock Enterprise Server utilise le port 9133.

Cliquez sur **Next** pour démarrer DeviceLock Enterprise Server et avancer jusqu'à l'écran suivant.

Si l'utilisateur actuel ne dispose pas d'un accès administratif complet à DeviceLock Enterprise Server (si celui-ci existe déjà et que vous effectuez une mise à jour), l'assistant de configuration ne pourra ni installer le service, ni appliquer les changements. Une erreur similaire peut aussi se produire dans le cas où l'utilisateur actuel ne dispose pas des privilèges administratifs sur l'ordinateur où l'installation de DeviceLock Enterprise Server a lieu.



Si vous avez saisi un nom d'utilisateur erroné pour le paramètre **This account** ou un mauvais mot de passe, DeviceLock Enterprise Server ne pourra pas démarrer.

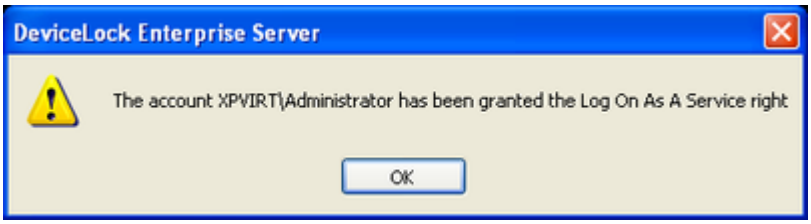
DeviceLock Enterprise Server - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

Le programme vous avertira si le compte utilisateur spécifié dans l'option **This account** n'est pas membre du groupe Domain Admins.

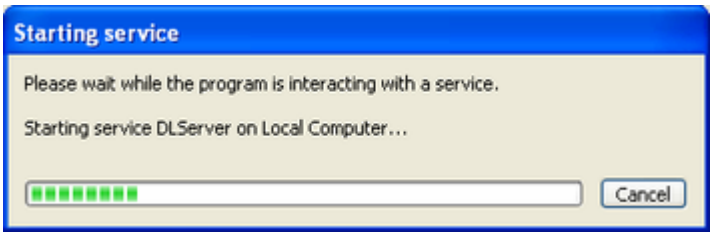
DeviceLock Enterprise Server
The account vm2000ad\test does not belong to the Domain Admins group.
Do you want to continue?
Yes
No

Vous pouvez continuer en appuyant sur **Yes**. Mais attention: dans ce cas, soit l'utilisateur en question doit avoir un accès administratif complet à toutes les instances en cours à distance de DeviceLock Services, soit DeviceLock Certificate (la clé publique) doit être installé sur chaque ordinateur équipé de DeviceLock Service.

Si le compte utilisateur spécifié dans l'option **This account** n'a pas le privilège système Log On As A Service, l'assistant l'accorde automatiquement. Ce privilège est nécessaire pour le démarrage du service au nom de l'utilisateur.

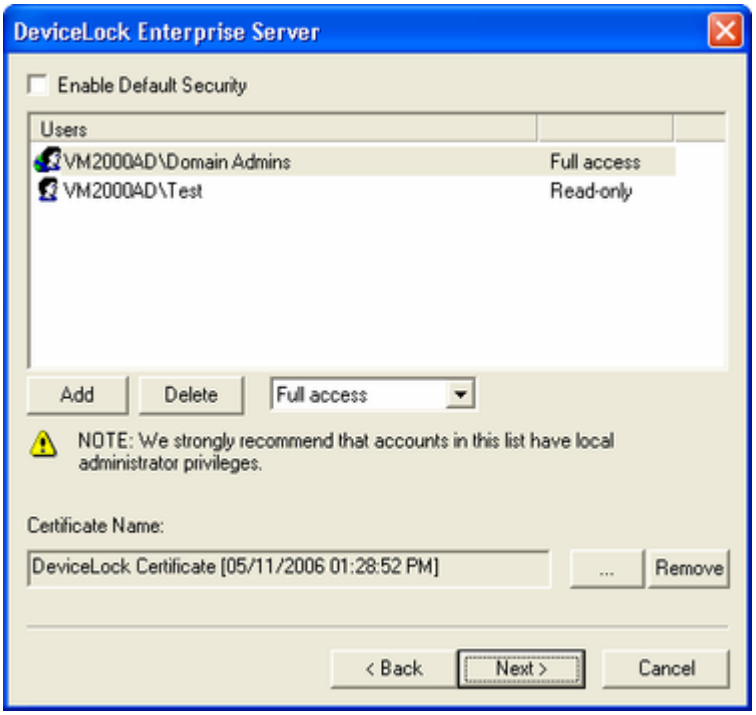


Si tous les paramètres de démarrage du service ont été correctement définis, l'assistant démarre DeviceLock Enterprise Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLServer on Local Computer...
Cancel

Le démarrage de DeviceLock Enterprise Server et l'affichage du deuxième écran de l'assistant peuvent prendre un certain temps (jusqu'à une minute).

Sur le deuxième écran, vous pouvez définir la liste des utilisateurs qui ont un accès administratif à DeviceLock Enterprise Server et installer DeviceLock Certificate (la clé privée).



Enable Default Security (Activer la sécurité par défaut)
Dans la configuration de sécurité par défaut, tous les utilisateurs bénéficiant d'un accès administratif local (autrement dit les membres du groupe local Administrators) peuvent se connecter à DeviceLock Enterprise Server avec une console de gestion et changer sa configuration ou créer des rapports.

Pour activer la sécurité par défaut, cochez la case **Enable Default Security**.

Si vous devez définir l'accès à DeviceLock Enterprise Server d'une façon plus détaillée, désactivez la sécurité par défaut en décochant la case **Enable Default Security**.

Vous devrez alors préciser les comptes autorisés (les utilisateurs et/ou les groupes) qui peuvent se connecter à DeviceLock Enterprise Server. Pour ajouter un nouvel utilisateur ou un nouveau groupe à la liste de comptes, cliquez sur le bouton **Add**. Vous pouvez ajouter plusieurs comptes en même temps.

Pour supprimer une entrée de la liste des comptes, utilisez le bouton **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Pour définir les actions qu'un utilisateur ou un groupe d'utilisateurs est en droit d'effectuer, définissez les droits correspondants:

- **Full access:** permet l'accès libre à DeviceLock Enterprise Server. Les utilisateurs peuvent changer la configuration et créer des rapports.

- **Change:** permet de changer l'accès à DeviceLock Enterprise Server. Les utilisateurs peuvent changer les paramètres, installer ou désinstaller DeviceLock Enterprise Server et lancer des rapports, mais ils ne peuvent pas ajouter de nouveaux utilisateurs à la liste des comptes autorisés susceptibles de se connecter à DeviceLock Enterprise Server ou changer les droits d'accès des utilisateurs existants dans cette liste.
- **Read-only:** permet un accès en lecture seule à DeviceLock Enterprise Server. Les utilisateurs peuvent créer des rapports et afficher les paramètres définis, mais ils ne peuvent rien modifier.

Remarque: Nous conseillons fortement d'accorder aux comptes figurant dans cette liste des privilèges d'administrateur local car, dans certains cas, il peut s'avérer nécessaire de disposer de droits d'accès à Windows Service Control Manager (SCM) et aux ressources de réseau partagées pour installer, mettre à jour et désinstaller DeviceLock Enterprise Server.

Certificate Name (Nom de certificat)
Vous aurez peut-être besoin d'installer la clé privée sur DeviceLock Enterprise Server pour activer l'identification à l'aide de DeviceLock Certificate.

Il existe deux méthodes d'identification de DeviceLock Enterprise Server sur les instances à distance de DeviceLock Services:

- **Identification par utilisateur**: DeviceLock Enterprise Server fonctionne dans le compte de l'utilisateur qui a un accès administratif complet à DeviceLock Service sur l'ordinateur distant. Pour plus d'informations sur le fonctionnement de DeviceLock Enterprise Server pour le compte de l'utilisateur, veuillez lire la description du paramètre Log on as.
- **Identification par DeviceLock Certificate**: Si l'utilisateur dont le compte exécute DeviceLock Server ne peut pas accéder à DeviceLock Service sur l'ordinateur distant, vous devez vous identifier à l'aide de DeviceLock Certificate.

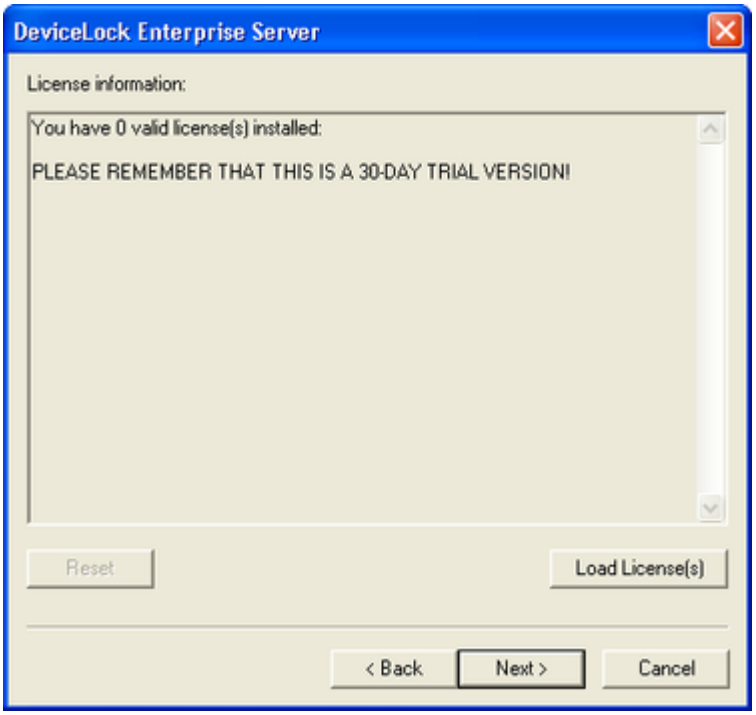
La clé publique doit être installée sur DeviceLock Service et la clé privée correspondante sur DeviceLock Enterprise Server.

Pour installer DeviceLock Certificate, appuyez sur le bouton **...**, et sélectionnez le fichier comportant une clé privée. Pour supprimer DeviceLock Certificate, appuyez sur le bouton **Remove**.

Pour plus de détails sur DeviceLock Certificate, veuillez vous reporter au chapitre DeviceLock Certificates de ce manuel.

Appuyez sur **Next** pour appliquer les modifications et avancer jusqu'à l'écran suivant de l'assistant de configuration.

Depuis cette page, vous pouvez charger vos licences DeviceLock.



License information (Informations de licence)
Si vous avez acheté une licence pour DeviceLock, vous devrez charger cette licence dans DeviceLock Enterprise Server.

DeviceLock Enterprise Server ne peut pas gérer plus de DeviceLock Services qu'il n'y a de licences. Par exemple, si vous avez une licence pour 100 ordinateurs mais qu'il y a 101 instances de DeviceLock Service en fonction sur votre réseau, DeviceLock Enterprise Server ne fonctionnera qu'avec les 100 premiers DeviceLock Services et ne prendra pas en compte le dernier.

Pour charger la licence, appuyez sur **Load License(s)** et sélectionnez le fichier de licence.

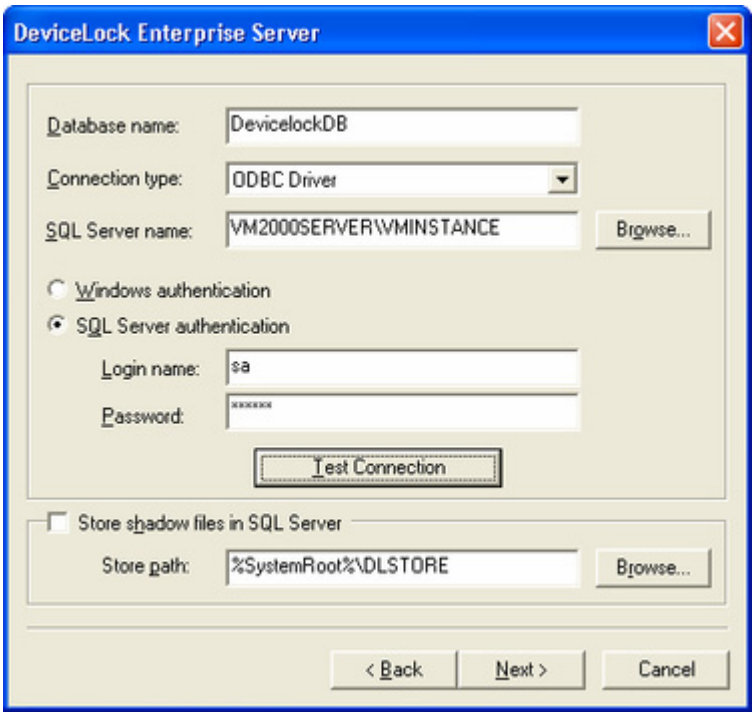
Vous pouvez charger plusieurs fichiers de licence en série, un à un.

Si aucune licence valide n'est chargée, DeviceLock Enterprise Server fonctionne en mode démo et ne pourra gérer que deux instances de DeviceLock Service.

Remarque: Si un ordinateur avec DeviceLock Service se déconnecte du réseau, DeviceLock Enterprise Server n'effectuera son remplacement qu'après un redémarrage ou après une durée de 6 heures.

Appuyez sur **Next** pour installer les licences et avancer jusqu'à l'écran suivant.

Sur le quatrième écran, vous pouvez configurer les paramètres de la base de données.



Database name (Nom de la base de données)
Vous devez spécifier le nom de la base de données qui sera utilisée, dans SQL Server, pour les données de DeviceLock Enterprise Server. Par défaut, le nom suggéré par l'assistant est **DeviceLockDB**.

Remarque: Il est déconseillé de créer manuellement une base de données avec le nom spécifié car l'assistant de configuration crée automatiquement la base de données ou utilise la base de données existante.

Connection type (Type de connexion)
Il existe deux manières de définir une connexion à un SQL Server.

1. **ODBC Driver**: saisissez le nom de SQL Server dans l'option **SQL Server name**, et sélectionnez le mode d'identification (Windows ou SQL Server).

   Le paramètre **SQL Server name** doit contenir non seulement le nom de l'ordinateur qui exécute SQL Server mais aussi le nom du SQL Server lui-même. Le nom du SQL Server est habituellement constitué de deux parties: le nom de l'ordinateur et le nom de l'instance, séparés par une barre oblique inverse (par exemple, computer\instance). Le nom de l'instance est parfois vide (par défaut), et vous pouvez utiliser le nom de l'ordinateur comme nom de SQL Server. Pour récupérer les noms de SQL Server disponibles sur votre réseau, cliquez sur **Browse**. (Vous devez avoir accès au registre à distance de l'ordinateur muni de SQL Server pour récupérer le nom de l'instance.)

Si le paramètre **SQL Server Name** est vide, c'est que SQL Server fonctionne sur le même ordinateur que DeviceLock Enterprise Server et que le nom de l'instance est vide (par défaut).

Pour établir une connexion à SQL Server, vous devez aussi configurer des paramètres d'identification.

Sélectionnez le paramètre **Windows authentification** pour vous identifier sur SQL Server avec le compte utilisé pour exécuter DeviceLock Enterprise Server.

Si le service a été activé avec le compte SYSTEM, et si SQL Server fonctionne sur l'ordinateur distant, le service ne pourra pas se connecter à SQL Server puisque l'utilisateur SYSTEM n'a pas les droits nécessaires pour accéder au réseau. Pour plus d'informations sur le fonctionnement de DeviceLock Enterprise Server pour l'utilisateur, veuillez lire la description du paramètre Log on as.

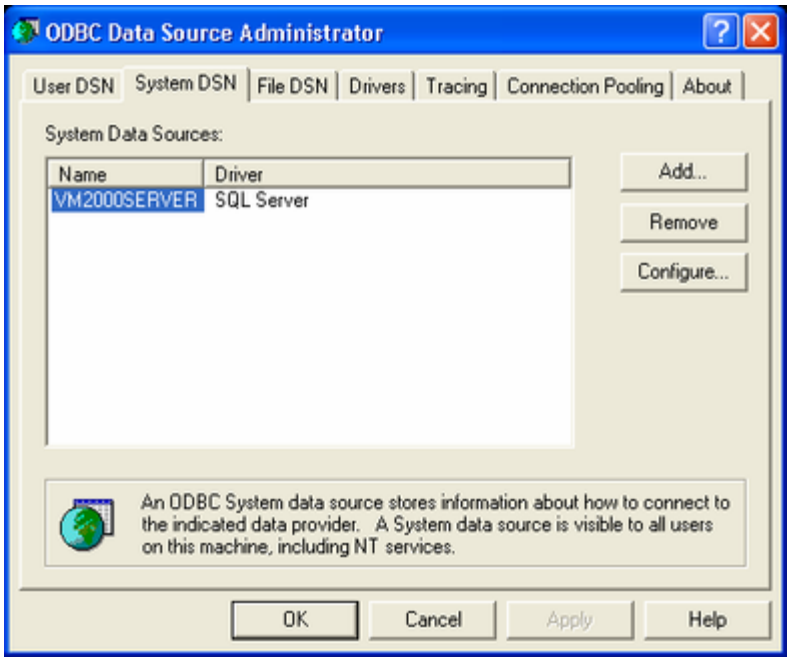
Sélectionnez le paramètre **SQL Server authentification** pour permettre à SQL Server de vérifier lui-même l'identification en exigeant le nom d'utilisateur et le mot de passe préalablement définis. Avant de sélectionner le paramètre **SQL Server authentification**, assurez-vous d'avoir configuré votre SQL Server pour l'identification en mode mixte.

Saisissez le nom d'utilisateur SQL (login) dans **Login name** et son mot de passe dans **Password**.

Remarque: Utilisez autant que possible l'identification Windows Authentification, nettement plus sécurisée que SQL Server Authentification.

2. **System Data Source**: sélectionnez la source de données système prédéfinie à partir de la liste **Data Source Name**.

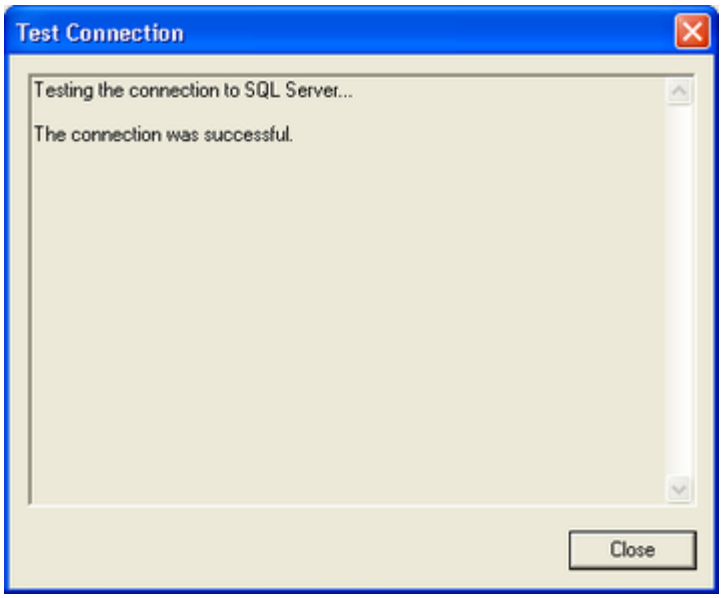
   Pour définir les sources de données, utilisez l'applet **Data Sources (ODBC)** à partir de **Panneau de Configuration** -> **Outils d'administration**.



Si vous avez choisi SQL Server Authentification dans la configuration de la source de données, renseignez aussi le nom d'utilisateur SQL (login) dans **Login name** et son mot de passe dans **Password**. Dans le cas contraire, ne renseignez pas ces champs.

Pour mettre à jour la liste **Data Source Name**, appuyez sur **Refresh**.

Une fois la connexion à SQL Server définie, vous voudrez peut-être la tester. Appuyez sur **Test Connection** pour vérifier que tous les paramètres sont définis correctement.



Veuillez noter que cette vérification ne porte que sur la connectivité et sur vos droits d'accès à SQL Server. Si la base de données fonctionne mal, ou si vos droits d'accès à cette base de données sont insuffisants, ces problèmes n'apparaîtront pas dans la boîte de dialogue **Test Connection**.

Si certains paramètres de connexion ont été mal renseignés, le système risque de vous signaler l'une des erreurs suivantes:

- **SQL Server does not exist or access denied**: vous avez spécifié un nom de SQL Server erroné dans le paramètre **SQL Server** ou l'ordinateur à distance qui exécute SQL Server n'est pas accessible. Vous avez peut-être spécifié le nom de l'ordinateur qui exécute SQL Server mais celui-ci a aussi un nom d'instance qu'il faut spécifier (par exemple, computer\instance).
- **Login failed for user 'COMPUTER_NAME$'**: vous avez choisi Windows Authentification mais le compte utilisateur utilisé pour l'exécution de DeviceLock Enterprise Server ne peut pas accéder à l'ordinateur qui exécute SQL Server. C'est peut-être que le service a démarré avec l'utilisateur SYSTEM, ou pour le compte d'un utilisateur qui n'a pas de privilèges d'administrateur local sur l'ordinateur distant du SQL Server.

- **Login failed for user 'user_name'**: vous avez sélectionné SQL Server Authentication et défini soit un nom d'utilisateur SQL (login), soit un mot de passe erroné. Veuillez noter que les utilisateurs SQL ne sont pas identiques aux utilisateurs Windows et que vous ne pouvez donc pas utiliser le compte habituel Windows pour le paramètre **Login name**. Les utilisateurs SQL n'existent que dans SQL Server et pour les administrer, vous devez utiliser une console d'administration de SQL Server (telle que Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection**: vous avez choisi SQL Server Authentication mais votre SQL Server n'accepte pas ce mode. Vous devez soit utiliser Windows Authentification, soit permettre à votre SQL Server l'utilisation du mode mixte (mode SQL Server et Windows Authentification).
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection**: la source de données que vous avez spécifiée dans le paramètre **Data Source Name** est configurée pour l'utilisation du mode SQL Server Authentication mais le paramètre **Login name** est vide.
- **Data source name not found and no default driver specified**: vous avez sélectionné **Data Source** dans la liste **Connection type** et spécifié un nom soit vide, soit inexistant dans le paramètre **Data Source Name**.

Store shadow files in SQL Server (Stocker des données binaries dans SQL Server)
Il est possible de stocker des données binaires soit dans SQL Server, soit sur le disque.

Pour stocker les données dans SQL Server, cochez la case **Store shadow files in SQL Server**.

Si vous avez décidé de stocker des données binaires dans SQL Server, il est recommandé d'accroître considérablement le paramètre de la taille supérieure de fichier pour le rapport de transaction de la base de données spécifié dans **Database name**. Dans le cas contraire, il est possible que SQL Server ne réussisse pas à gérer une telle somme de données (plusieurs centaines de méga-octets) en une seule transaction. Il est aussi recommandé d'augmenter la quantité totale de mémoire à la disposition de SQL Server, et d'activer la fonctionnalité PAE (extension d'adresse physique).

Pour plus d'informations sur le réglage fin de SQL Server pour le stockage de grandes quantités de données, vous pouvez lire l'article disponible sur le site Web de Microsoft:
http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/rdbmspft.mspx.

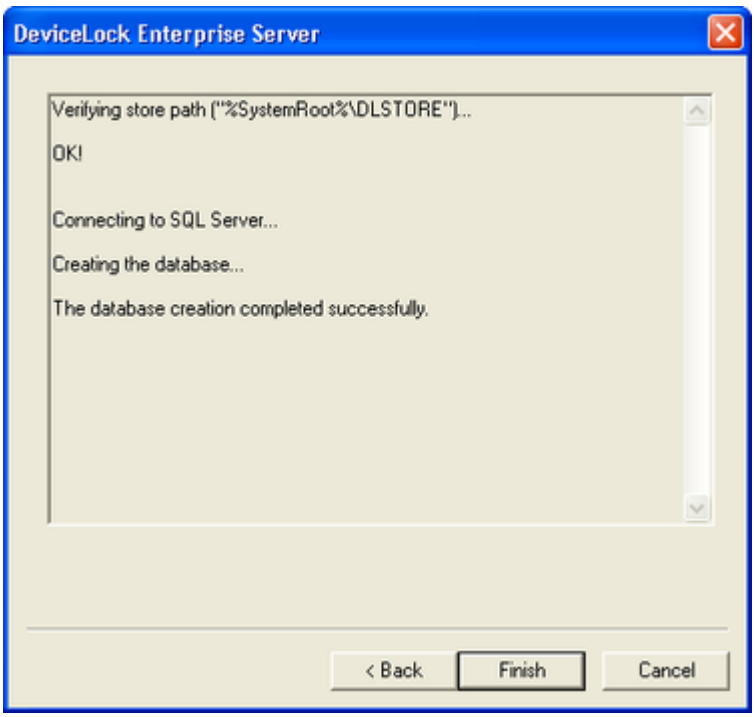
Pour stocker des données sur le disque, décochez la case **Store shadow files in SQL Server**. Dans ce cas, SQL Server ne contient que des liens vers les données binaires, avec quelques informations supplémentaires.

Lorsqu'ils sont stockés sur le disque, les fichiers de données sont identifiés grâce au chemin spécifié dans le paramètre **Store path**. Pour choisir le dossier où seront stockés les fichiers, utilisez le bouton **Browse**.

Vous pouvez aussi définir la ressource de réseau partagée (p. ex. \\server\dlstore) qui servira de lieu de stockage. Attention: le compte utilisateur servant à exécuter DeviceLock Enterprise Server doit avoir un accès complet à cette ressource de réseau.

Remarque: Il est conseillé de stocker les données binaires sur le disque.

Appuyez sur **Next** pour appliquer les modifications et avancer jusqu'à l'écran suivant.



L'ordinateur peut mettre un certain temps à créer la base de données spécifiée dans **Database name** si celle-ci n'existe pas encore sur ce SQL Server. Si la base de données existe déjà et possède un format approprié (si elle a été créée par DeviceLock Enterprise Server), DeviceLock Enterprise Server conserve toutes les données existantes et utilise cette base de données.

Remarque: Si nécessaire, DeviceLock met automatiquement à jour la base de données à la version la plus récente.

Si certains paramètres de l'écran précédent de l'assistant ont été mal renseignés, le système risque de vous signaler l'une des erreurs suivantes:

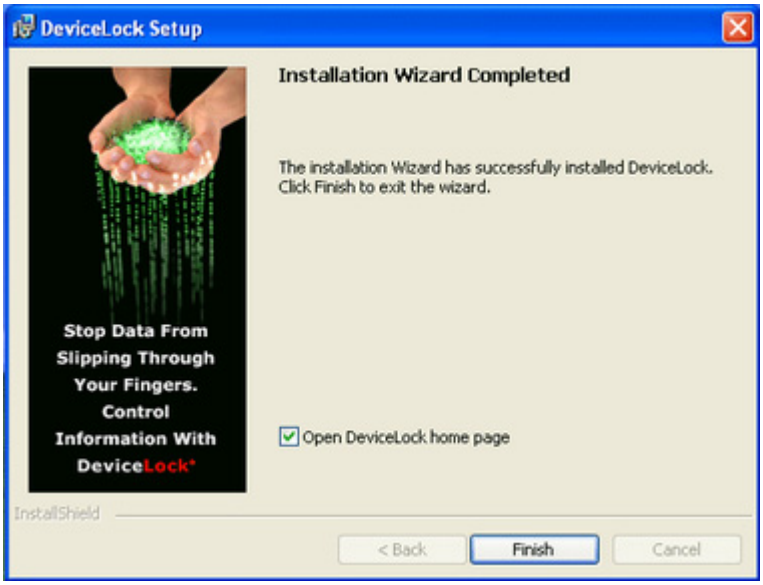
- **[2] The system cannot find the file specified**: DeviceLock Enterprise Server a été configuré pour le stockage de données sur le disque mais le chemin spécifié dans **Store path** est erroné. Si vous avez spécifié une ressource de réseau partagée, il est possible que cette ressource de réseau soit inaccessible.
- **Failed to verify store path. [5] Access is denied**: le chemin spécifié dans le paramètre **Store path** est exact, mais le compte utilisé pour l'exécution de DeviceLock Enterprise Server n'a pas un accès complet aux fichiers via ce chemin.
- **CREATE DATABASE permission denied in database 'name'**: le compte (login) utilisé pour la connexion à SQL Server n'a pas les privilèges nécessaires pour créer la base de données. Le login doit avoir au moins le rôle de serveur dbcreator (voir **Server Roles** dans **Login Properties** de Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context**: le compte (login) utilisé pour la connexion à SQL Server n'a pas accès à la base de données existante. Le login doit être lié à cette base de données (voir **User Mapping** dans **Login Properties** de Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'**: le compte (login) utilisé pour la connexion à SQL Server ne dispose pas d'un accès en lecture/écriture à la base de données existante. Le login doit avoir au moins les rôles db_datareader et db_datawriter dans la base de données (voir **User Mapping** dans **Login Properties** de Microsoft SQL Server Management Studio).
- **Invalid object name 'name'**: la base de données spécifiée dans le paramètre **Database name** existe déjà dans ce SQL Server mais le format n'est pas le bon. Cette erreur apparaît lorsque vous essayez d'utiliser une base de données qui n'a pas été créée par DeviceLock Enterprise Server ou lorsque cette base de données est corrompue.
- **DeviceLock Database has an unsupported format**: la base de données spécifiée dans le paramètre **Database name** existe déjà mais n'est plus à jour. Le format de cette base de données existante n'est pas pris en charge, si bien qu'il est impossible de le transformer automatiquement dans le nouveau format. Vous devez soit utiliser une autre base de données, soit en créer une nouvelle.
- **DeviceLock Database has a format that is not supported by the current server version**: la base de données spécifiée dans le paramètre **Database name** existe déjà mais a été créée avec une version plus récente de DeviceLock Enterprise Server. Utilisez la version la plus récente de DeviceLock Enterprise Server ou une autre base de données (ou créez une nouvelle base de données).

Certaines des erreurs de connexion SQL Server décrites ci-dessus peuvent aussi s'afficher ici.

Utilisez le bouton **Back** pour revenir à la page précédente et faire les changements qui s'imposent.

S'il n'y a pas d'erreurs, appuyez sur **Finish** pour fermer l'assistant et continuer la procédure d'installation.

Dès que le programme de configuration a terminé l'installation de DeviceLock, il vous propose de visiter le site Web de DeviceLock.



Décochez la case **Open DeviceLock home page** si vous ne désirez pas visiter le site Web de DeviceLock. Cliquez sur le bouton **Finish** pour terminer l'installation.

Remarque: Pour désinstaller DeviceLock, effectuer l'une ou l'autre des actions suivantes:

Utilisez l'option **Ajouter ou supprimer des programmes** du panneau de commande pour supprimer **DeviceLock**.
- OU -
Cliquez sur **Démarrer**, sélectionnez **Tous les programmes**, puis **DeviceLock**, et cliquez sur **Remove DeviceLock**.

Installation de DeviceLock Content Security Server

Pour installer DeviceLock Content Security Server, procédez comme suit:

- Etape 1. Préparation de l'installation
- Etape 2. Démarrage de l'installation

- Etape 3. Configuration de DeviceLock Content Security Server et installation proprement dite.

Etape 1: Préparation de l'installation

Avant d'installer DeviceLock Content Security Server, tenez compte des importantes remarques suivantes:

- L'ordinateur sur lequel vous installez DeviceLock Content Security Server doit remplir les conditions suivantes:

Système d'exploitation	Microsoft Windows NT 4.0 Service Pack (SP) 6, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, ou Windows 7. L'installation est prise en charge sur les versions tant 32-bit que 64-bit du système d'exploitation.
Navigateur web	Windows Internet Explorer version 4.0 ou ultérieure doit être installé sur les ordinateurs sous Windows NT 4.0 SP 6.
Espace sur le disque dur	19 Mo

- Vous devez disposer de privilèges d'administrateur pour installer DeviceLock Content Security Server.
- Pour des performances et une fiabilité optimales, nous recommandons d'installer DeviceLock Enterprise Server et DeviceLock Content Security Server sur plusieurs ordinateurs.
- L'utilisation de DeviceLock Content Security Server nécessite l'achat d'une licence Search Server spéciale. Vous pouvez utiliser la même licence sur un nombre illimité d'ordinateurs exécutant DeviceLock Content Security Server. Le modèle de gestion de licence de Search Server dépend du nombre d'entrées de journal à indexer pour l'exploration systématique de texte. Chaque licence permet à Search Server d'indexer 1000 entrées des journaux de réplication (journal de réplication et journal de réplication supprimé), et 5000 entrées de chacun des autres journaux (journal d'audit, journal de serveur et journal de surveillance). En fonction du nombre réel d'entrées de journal sur vos DeviceLock Enterprise Servers, vous pouvez acheter le nombre de licences de votre choix. Si vous utilisez plusieurs licences Search Server, le nombre d'entrées de journal indexables est la somme de celles correspondant à chaque licence. La période d'essai de DeviceLock Content Security Server est de 30 jours. Pendant la période d'essai, Search Server peut indexer 2000 entrées à partir des journaux de réplication et 10 000 entrées à partir des autres journaux.
- Si votre réseau comporte plusieurs DeviceLock Enterprise Servers, vous pouvez aussi installer plusieurs DeviceLock Content Security Servers pour répartir la charge. Cependant, cette approche n'a pas de sens si tous ces DeviceLock Enterprise Servers sont connectés au même Microsoft SQL Server (autrement dit pas en mode «MANY-TO-ONE»).

- Si plusieurs DeviceLock Content Security Servers sont installés, chaque Search Server doit disposer de son propre indice de recherche. Par conséquent, il faut se connecter à chacun des DeviceLock Content Security Servers et effectuer la même recherche sur chaque Search Server pour obtenir l'ensemble des résultats correspondant aux données stockées sur tous les DeviceLock Enterprise Servers.
- Nous vous conseillons fortement de fermer tous les programmes Windows avant de lancer la configuration.

Etape 2. Démarrage de l'installation

Utilisez cette procédure pour lancer le processus d'installation.

Pour lancer l'installation

1. Ouvrez le fichier **DeviceLock.zip**, puis double-cliquez sur le fichier **setup_dlcss.exe** pour lancer l'installateur.

   L'installateur doit être lancé sur chacun des ordinateurs sur lesquels vous souhaitez installer DeviceLock Content Security Server.

2. Suivez les instructions de l'installateur.
3. Dans la page **License Agreement**, lisez l'accord de licence et cliquez sur **Accept the terms in the licence agreement** pour accepter les termes et conditions de l'accord de licence et procéder à l'installation.
4. Dans la page **Customer Information** (informations du client), saisissez votre nom d'utilisateur et celui de votre organisation et cliquez sur le bouton **Next** (suivant).
5. Dans la page **Destination Folder**, acceptez le répertoire d'installation par défaut ou cliquez sur **Change** pour modifier le chemin à votre convenance. Cliquez sur **Next**.

   Par défaut, le répertoire d'installation est %ProgramFiles%\DeviceLock\DeviceLock Content Security Server.

6. Dans la page **Ready to Install the Program** (prêt pour l'installation), cliquez sur **Install** pour démarrer l'installation.

   L'assistant DeviceLock Content Security Server démarre.

   Si vous effectuez une mise à jour ou une simple réinstallation de DeviceLock Content Security Server, et souhaitez conserver le paramétrage actuel, inutile de reprendre cet assistant: cliquez sur **Cancel** pour fermer l'assistant et conserver en l'état les paramètres préexistants.

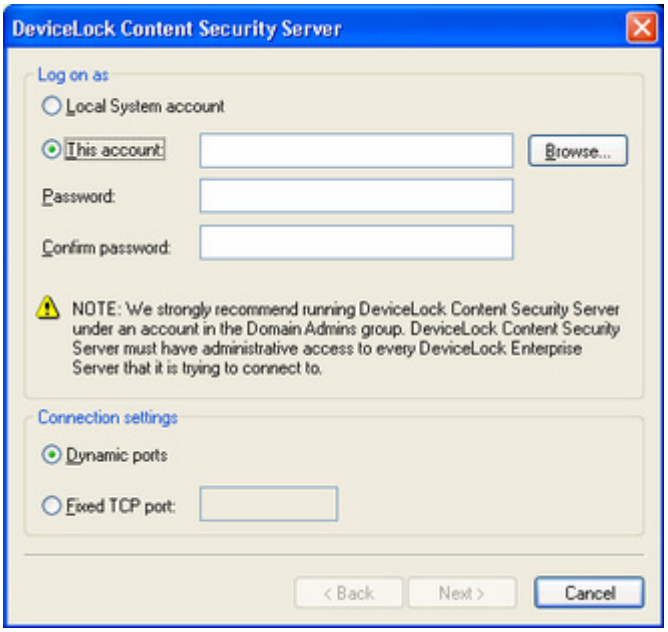
   Dans le cas où il vous faudrait changer certains paramètres mais en garder d'autres, éditez uniquement les paramètres nécessaires et passez par tous les écrans de l'assistant jusqu'au bouton **Finish** de la dernière page.

Remarque: Si vous installez DeviceLock Content Security Server pour la première fois (il n'y a pas encore de paramètres sur cet ordinateur) et que vous annulez l'assistant de configuration au démarrage, l'installateur ne pourra pas installer DeviceLock Content Security Server; il vous faudra donc relancer l'assistant de configuration.

Etape 3. Configuration de DeviceLock Content Security Server et installation proprement dite.

L'assistant DeviceLock Content Security Server s'ouvre automatiquement lors du processus d'installation. L'assistant vous guide parmi les paramètres à configurer pour utiliser DeviceLock Content Security Server.

La première page de l'assistant a l'aspect suivant:


DeviceLock Content Security Server
Log on as
Local System account
This account:
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Content Security Server under an account in the Domain Admins group. DeviceLock Content Security Server must have administrative access to every DeviceLock Enterprise Server that it is trying to connect to.
Connection settings
Dynamic ports
Fixed TCP port:
< Back
Next >
Cancel

Cette page sert à configurer les options de démarrage de DeviceLock Content Security Server.

Log on as (Se connecter en tant que)
Commencez par choisir un compte de démarrage de DeviceLock Content Security Server. Comme bien d'autres services Windows, le service DeviceLock Content Security Server peut démarrer sous le compte particulier du système local (l'utilisateur SYSTEM), quel que soit l'utilisateur considéré.

Pour démarrer le service avec le compte SYSTEM, choisissez l'option **Local System account**. Notez que le processus qui utilise le compte SYSTEM ne peut pas accéder aux ressources de réseau partagées, et s'identifie auprès des ordinateurs distants en tant qu'utilisateur anonyme. C'est pourquoi DeviceLock Content Security Server, configuré pour fonctionner avec le compte SYSTEM, n'est pas en mesure d'accéder au DeviceLock Enterprise Server exécuté sur l'ordinateur distant et doit utiliser DeviceLock Certificate pour s'identifier auprès de lui.

Pour plus d'informations sur les méthodes d'identification, veuillez vous reporter à la description du paramètre Certificate Name.

Pour démarrer le service au nom de l'utilisateur, choisissez l'option **This account**, puis saisissez le nom du compte et le mot de passe. Il est conseillé d'utiliser un compte d'utilisateur disposant de privilèges d'administration sur tous les ordinateurs qui exécutent DeviceLock Enterprise Server. Dans le cas contraire, il vous faudra utiliser l'identification DeviceLock Certificate.

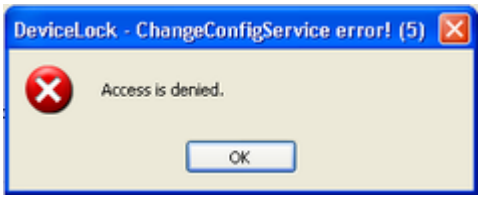
Si vous installez DeviceLock Content Security Server dans l'environnement de domaine, nous vous conseillons d'utiliser un compte d'utilisateur appartenant au groupe Domain Admins. Etant donné que Domain Admins fait partie du groupe local Administrators sur chacun des ordinateurs du domaine, tous les membres de Domain Admins bénéficieront d'un accès libre à DeviceLock Enterprise Server sur chacun des ordinateurs.

Et n'oubliez pas que si Default Security est désactivé sur les DeviceLock Enterprise Server distants, le compte de l'utilisateur mentionné dans le paramètre **This account** doit aussi figurer dans la liste des Server Administrators bénéficiant au moins de droits **Read-only** sur ce DeviceLock Enterprise Server. Dans le cas contraire, il vous faudra utiliser l'identification par DeviceLock Certificate.

Connection settings (Paramètres de connexion)
Vous pouvez ordonner à DeviceLock Content Security Server d'utiliser un port TCP fixe pour la communication avec la console d'administration, ce qui simplifie la configuration d'un pare-feu, en saisissant le numéro de port dans **Fixed TCP port**. Pour utiliser les ports dynamiques pour la communication RPC, cliquez sur **Dynamic ports**. Par défaut, DeviceLock Content Security Server utilise le port 9134.

Cliquez sur **Next** pour démarrer DeviceLock Content Security Server et passer à l'écran suivant.

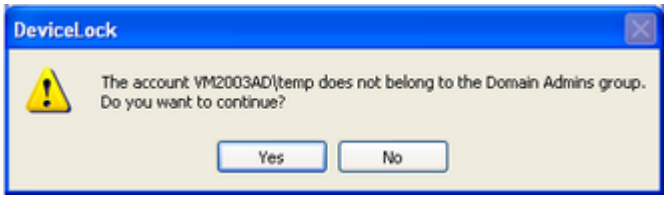
Si l'utilisateur actuel ne dispose pas d'un accès administratif complet à DeviceLock Content Security Server (si celui-ci existe déjà et que vous effectuez une mise à jour), l'assistant de configuration ne pourra ni installer le service, ni appliquer les changements. Une erreur similaire peut aussi se produire dans le cas où l'utilisateur actuel ne dispose pas des privilèges administratifs sur l'ordinateur concerné par l'installation de DeviceLock Content Security Server.



Si vous avez saisi un nom d'utilisateur erroné pour le paramètre **This account** ou un mauvais mot de passe, DeviceLock Content Security Server ne pourra pas démarrer.

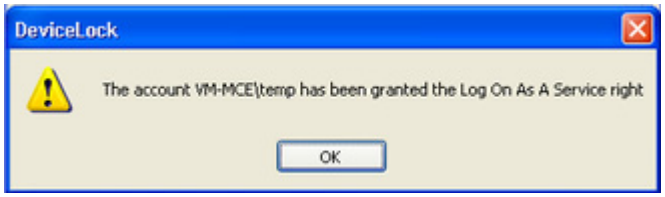
DeviceLock - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

Le programme vous avertira si le compte utilisateur spécifié dans l'option **This account** n'est pas membre du groupe Domain Admins.

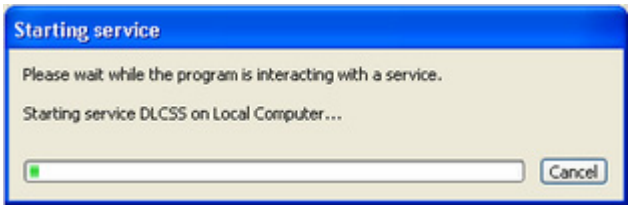


Vous pouvez continuer en appuyant sur **Yes**. Mais attention: dans ce cas, soit l'utilisateur en question doit disposer de droits d'administration pour tous les DeviceLock Enterprise Servers distants, soit un DeviceLock Certificate (une clé privée) doit être installé sur chaque ordinateur équipé de DeviceLock Enterprise Server.

Si le compte utilisateur spécifié dans l'option **This account** n'a pas le privilège système Log On As A Service, l'assistant l'accorde automatiquement. Ce privilège est nécessaire pour le démarrage du service au nom de l'utilisateur.

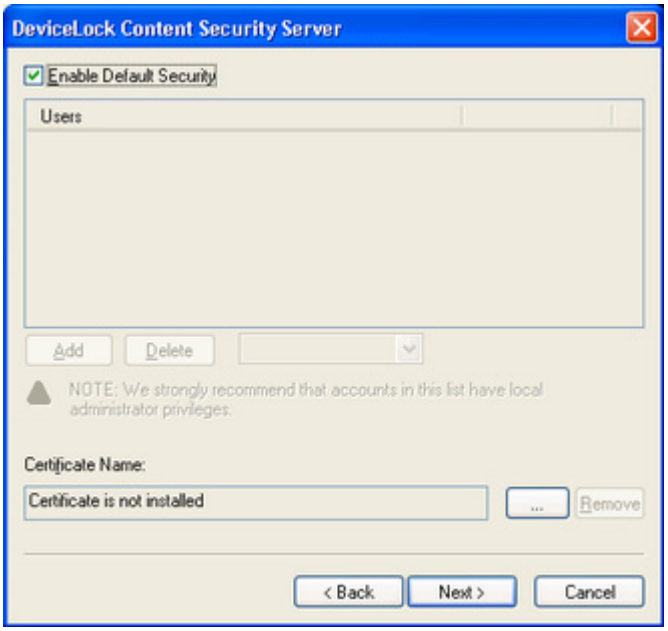


Si tous les paramètres de démarrage du service sont correctement définis, l'assistant démarre DeviceLock Content Security Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLCSS on Local Computer...
Cancel

Le démarrage de DeviceLock Content Security Server et l'affichage du deuxième écran de l'assistant peuvent prendre un certain temps (jusqu'à une minute).

Le deuxième écran de l'assistant a l'aspect suivant:



Sur cet écran, vous pouvez définir la liste des utilisateurs qui ont un accès administratif à DeviceLock Content Security et installer DeviceLock Certificate (la clé privée).

Enable Default Security (Activation de la sécurité par défaut)
Dans la configuration de sécurité par défaut, tous les utilisateurs bénéficiant de privilèges d'administrateur local (autrement dit les membres du groupe local Administrators) peuvent se connecter à DeviceLock Content Security Server avec une console de gestion et changer sa configuration ou lancer des recherches.

Pour activer la sécurité par défaut, cochez la case **Enable Default Security**.

Pour définir l'accès à DeviceLock Content Security Server d'une façon plus détaillée, désactivez la sécurité par défaut en décochant la case **Enable Default Security**.

Vous devrez alors préciser les comptes (utilisateurs et/ou groupes) autorisés à se connecter à DeviceLock Content Security Server. Pour ajouter un nouvel utilisateur ou un nouveau groupe à la liste de comptes, cliquez sur **Add**. Vous pouvez ajouter plusieurs comptes en même temps.

Pour supprimer un enregistrement de la liste des comptes, utiliser le bouton **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Pour définir les actions qu'un utilisateur ou un groupe d'utilisateurs est en droit d'effectuer, définissez les droits correspondants:

- **Full access**: permet l'accès libre à DeviceLock Content Security Server. Les utilisateurs peuvent changer les paramètres et lancer des recherches.

- **Change**: permet de modifier l'accès à DeviceLock Content Security Server. Les utilisateurs peuvent changer les paramètres, installer ou désinstaller DeviceLock Content Security Server et lancer des recherches, mais ils ne peuvent pas ajouter de nouveaux utilisateurs à la liste des comptes autorisés à se connecter à DeviceLock Content Security Server ou changer les droits d'accès des utilisateurs existants dans cette liste.
- **Read-only**: permet un accès en lecture seule à DeviceLock Content Security Server. Les utilisateurs peuvent lancer des recherches et afficher les paramètres, mais ils ne peuvent rien modifier ni créer un nouvel indice de Search Server.

Remarque: Nous conseillons fortement d'accorder aux comptes figurant dans cette liste des privilèges d'administrateur local car, dans certains cas, il peut s'avérer nécessaire de disposer de droits d'accès à Windows Service Control Manager (SCM) et aux ressources de réseau partagées pour installer, mettre à jour et désinstaller DeviceLock Content Security Server.

Certificate Name (Nom de certificat)
Vous aurez peut-être besoin d'installer la clé privée sur DeviceLock Content Security Server pour activer l'identification par DeviceLock Certificate.

Il existe deux méthodes d'identification de DeviceLock Content Security Server sur les instances à distance :

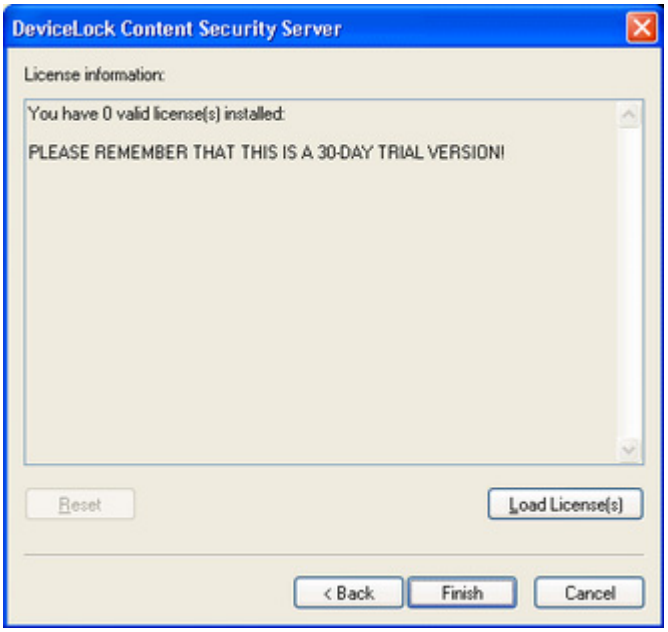
- **Identification par utilisateur**: DeviceLock Content Security Server fonctionne dans le compte de l'utilisateur qui a un accès administratif complet à DeviceLock Enterprise Server sur l'ordinateur distant. Pour en savoir plus sur le fonctionnement de DeviceLock Content Security Server pour le compte de l'utilisateur, veuillez lire la description du paramètre Log on as.
- **Identification par DeviceLock Certificate**: Si l'utilisateur dont le compte exécute DeviceLock Content Security Server ne peut pas accéder à DeviceLock Enterprise Server sur l'ordinateur distant, vous devez vous identifier par DeviceLock Certificate.
  La même clé privée doit être installée sur DeviceLock Enterprise Server et sur DeviceLock Content Security Server.

Pour installer un DeviceLock Certificate, appuyez sur le bouton ..., et sélectionnez le fichier comportant une clé privée. Pour supprimer un DeviceLock Certificate, cliquez sur **Remove**.

Pour plus de détails sur DeviceLock Certificate, veuillez vous reporter au chapitre DeviceLock Certificates de ce manuel

Appuyez sur **Next** pour appliquer les modifications et passer à l'écran suivant de l'assistant de configuration.

La page finale de l'assistant a l'aspect suivant:



Cette page permet de télécharger vos licences DeviceLock Content Security Server.

License information (Informations de licence)
Si vous avez acheté une licence Search Server, vous devrez charger cette licence dans DeviceLock Content Security Server.

Pour charger la licence, cliquez sur **Load License(s)** et sélectionnez le fichier de licence. Vous pouvez charger un à un plusieurs fichiers de licence.

La période d'essai de DeviceLock Content Security Server est de 30 jours.

Cliquez sur **Finish** pour fermer l'assistant et continuer le processus d'installation. Ensuite, cliquez sur **Finish** dans la page **Installation Wizard Completed** pour terminer l'installation. Cette page permet d'accéder à la page d'accueil de DeviceLock Content Security Server. Cette option est sélectionnée par défaut.

Remarque: Pour désinstaller DeviceLock Content Security Server, effectuer l'une ou l'autre des actions suivantes:

Utilisez l'option **Ajouter ou supprimer des programmes** du panneau de commande pour supprimer **DeviceLock Content Security Server**.
- OU -
Cliquez sur **Démarrer**, sélectionnez **Tous les programmes**, puis **DeviceLock**, et cliquez sur **Remove DeviceLock Content Security Server**.

DeviceLock Certificates

Présentation

Un DeviceLock Certificate est un certificat cryptographique composé de deux clés (la paire de clés): la clé privée et la clé publique.

- La clé privée doit être stockée sur l'ordinateur de l'administrateur et seul celui-ci doit pouvoir y accéder. La clé privée peut aussi être installée sur DeviceLock Enterprise Server et DeviceLock Content Security Server.

  Remarque: Vérifiez que les utilisateurs sans privilèges d'administrateur ne peuvent pas accéder à la clé privée.

- La clé publique est installée sur chacun des ordinateurs qui exécutent DeviceLock Service. Si la clé publique n'a pas été installée de manière préalable sur l'ordinateur de l'utilisateur, il n'est pas possible d'utiliser la fonction de Temporary white list, ni l'identification par DeviceLock Certificate de DeviceLock Enterprise Server.

Création de DeviceLock Certificates

L'outil de création de DeviceLock Certificates permet de générer des DeviceLock Certificates.

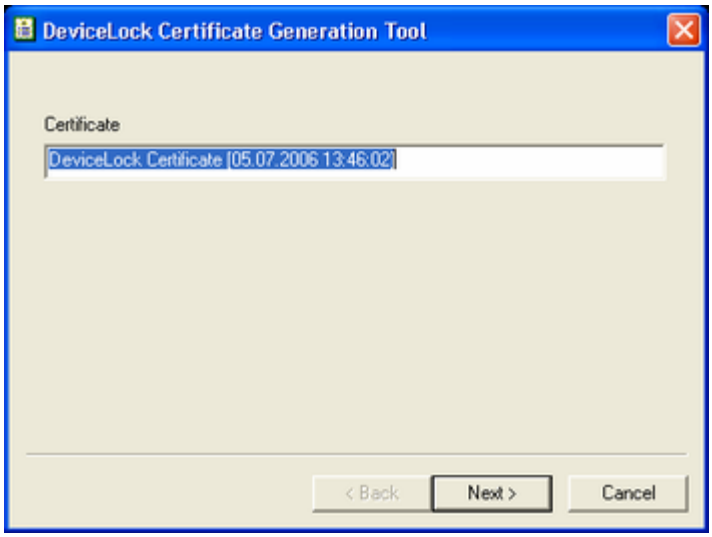
Nous vous conseillons de ne générer qu'un seul DeviceLock Certificate et d'installer sa clé publique sur tous les ordinateurs des utilisateurs. La génération et l'installation d'un nouveau certificat n'est nécessaire que si la clé privée est vulnérable (volée, par exemple) ou perdue.

Pour exécuter l'outil de génération de certificats, choisissez l'élément **Certificate Generation Tool** du menu **File** de DeviceLock Enterprise Manager. Pour exécuter l'outil de génération de certificats à partir de DeviceLock Management Console (le module MMC) ou de DeviceLock Group Policy Manager, utilisez le menu contextuel accessible par clic droit de la souris.

L'outil de génération de certificats s'exécutera automatiquement lorsque vous installez des consoles d'administration de DeviceLock sur un ordinateur d'administrateur sans DeviceLock Certificate.

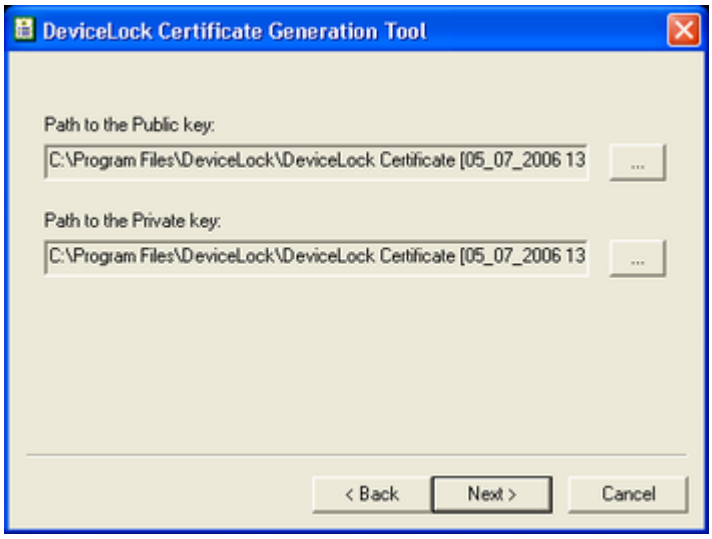
Pour générer la paire de clés, deux étapes simples sont nécessaires:

1. Définir le nom de DeviceLock Certificate.



L'outil de génération de certificats génère automatiquement un nom en fonction de la date et de l'heure considérés, mais vous pouvez en saisir un autre.

2. Définir le chemin et les noms de fichier des clés privée et publique.



Dès que le DeviceLock Certificate est généré, vous pouvez commencer à installer la clé publique sur les ordinateurs des utilisateurs.

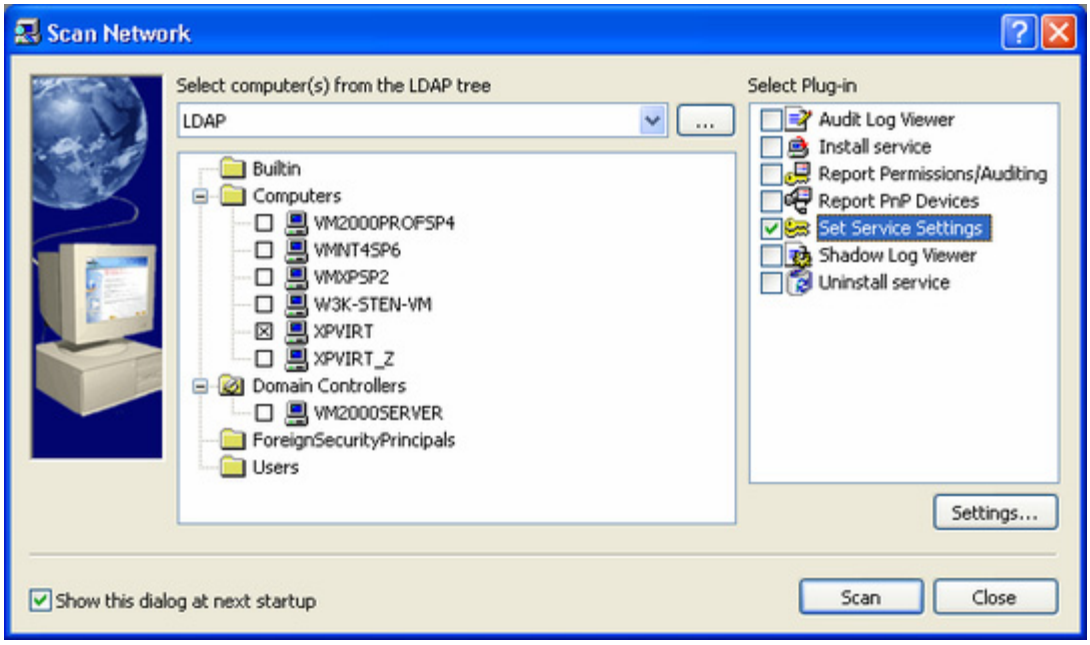
Remarque: Un DeviceLock Certificate récemment généré n'est pas automatiquement installé sur les ordinateurs à partir de l'outil de génération de certificats. Vous devez l'installer manuellement via la console de gestion de DeviceLock.

Installation et suppression de DeviceLock Certificates

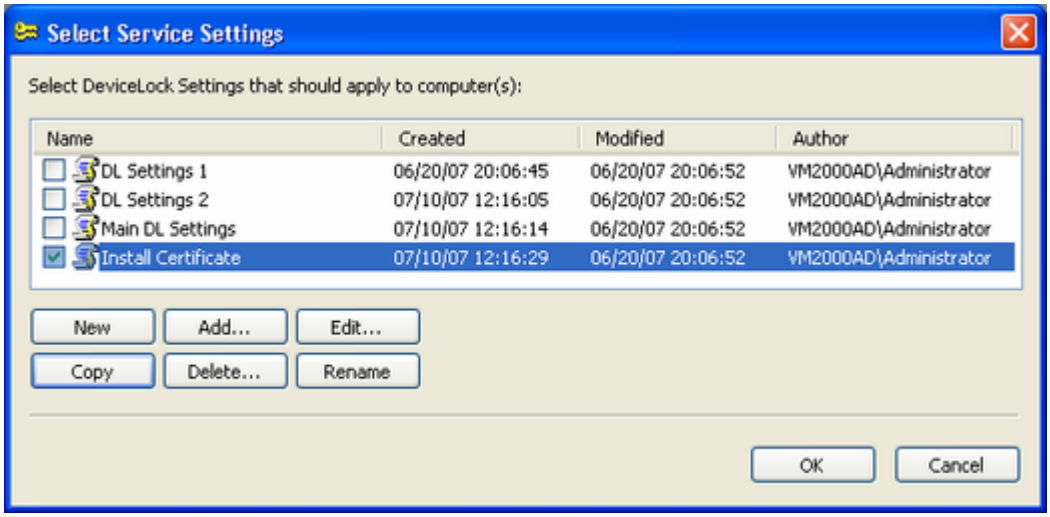
Pour installer ou supprimer la clé publique sur ou à partir d'ordinateurs utilisateur exécutant DeviceLock Services, n'importe quelle console d'administration de DeviceLock peut être utilisée.

- DeviceLock Enterprise Manager

  Dans la boîte de dialogue **Scan Network**, sélectionnez les ordinateurs sur lesquels ou à partir desquels vous voulez installer ou supprimer la clé publique, et sélectionnez l'extension **Set Service Settings**.



Appuyez sur **Settings** ou double-cliquez sur l'entrée de l'extension pour ouvrir la boîte de dialogue de configuration.

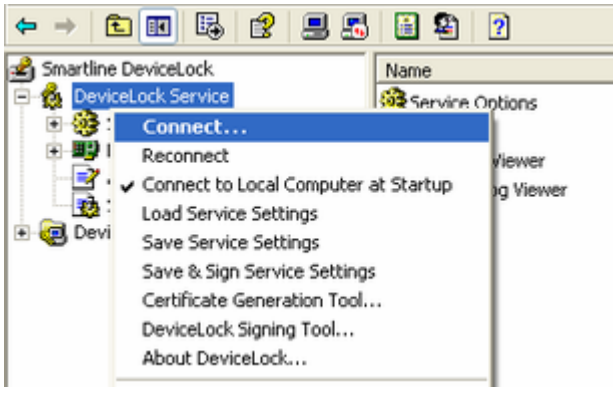


Créez le nouveau fichier XML ou utilisez le fichier préexistant pour définir la politique nécessaire à l'installation ou à la suppression du certificat. Mettez le fichier en surbrillance dans la liste et appuyez sur le bouton **Edit** pour modifier la politique comme indiqué dans le chapitre suivant (ci-dessous). Lorsque vous avez terminé de modifier la politique, choisissez un fichier dans la liste et cochez la case qui se situe à côté.

Appuyez sur **OK** pour fermer la fenêtre de configuration, puis appuyez sur le bouton **Scan** dans la fenêtre **Scan Network** pour démarrer la procédure d'installation ou de suppression de DeviceLock Certificate.

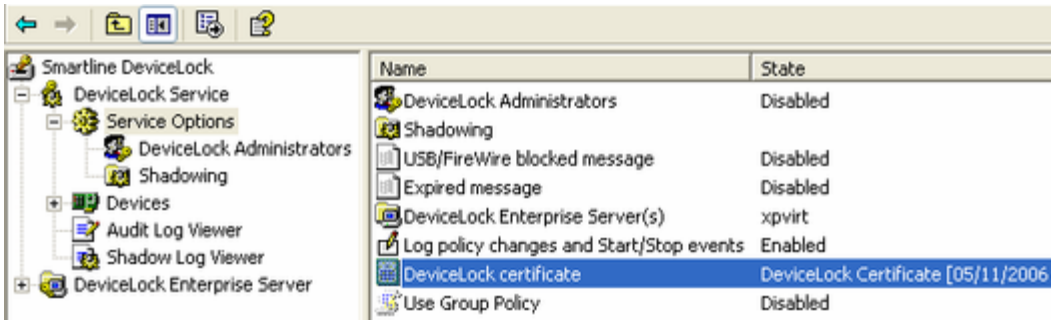
- DeviceLock Management Console, DeviceLock Group Policy Manager et DeviceLock Service Settings Editor

  Si vous utilisez DeviceLock Management Console (le module MMC intégré), vous devez tout d'abord le connecter à l'ordinateur qui exécute DeviceLock Service. Utilisez le menu contextuel accessible par simple clic droit de votre souris.



Si vous utilisez DeviceLock Group Policy Manager, il est inutile de se connecter à un ordinateur, puisqu'il se connecte au Group Policy Object. Il n'est pas non plus nécessaire de se connecter à l'ordinateur lorsque vous modifiez la politique dans le fichier XML avec DeviceLock Service Settings Editor.

Activez l'élément **Service Options**.



Double-cliquez sur le paramètre **DeviceLock Certificate** pour ouvrir la boîte de dialogue de configuration.

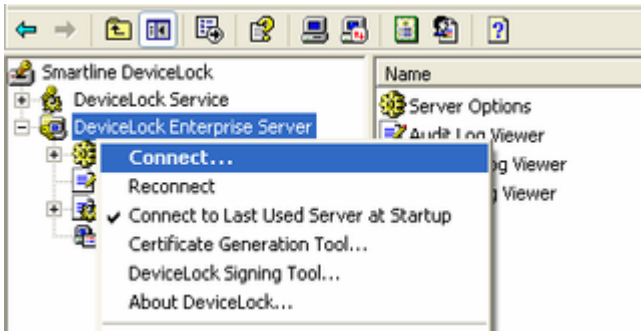
Renseignez le chemin d'accès de la clé publique dans le paramètre **Certificate Name** si vous voulez installer le certificat. Vous pouvez utiliser le bouton **...** pour sélectionner le fichier avec la clé publique.

Pour supprimer la clé publique, utilisez le bouton **Remove**.

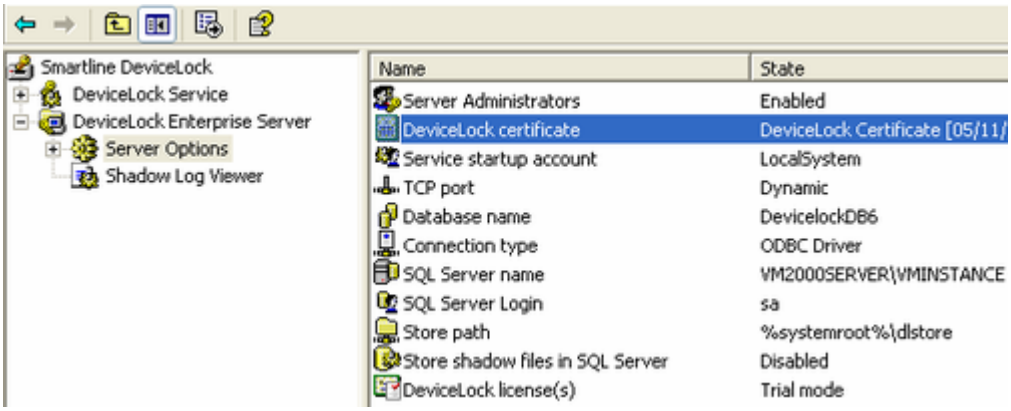
Appuyez sur **OK** pour fermer la boîte de dialogue de configuration et appliquer les modifications.

Pour installer la clé privée sur DeviceLock Enterprise Server et DeviceLock Content Security Server ou l'en supprimer, vous pouvez utiliser DeviceLock Management Console (le module MMC intégré).

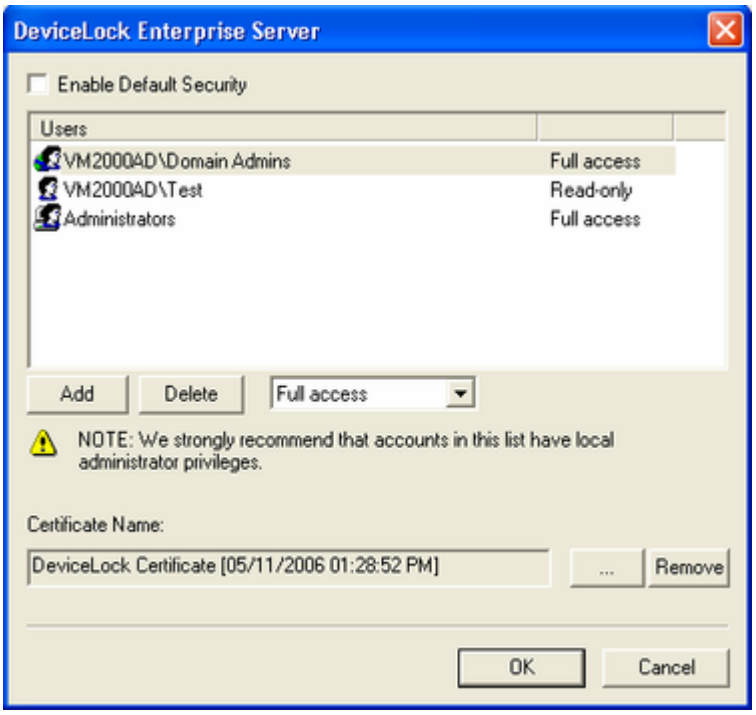
Vous devez connecter DeviceLock Management Console à l'ordinateur qui exécute DeviceLock Enterprise Server ou DeviceLock Content Security Server. Utilisez le menu contextuel accessible par simple clic droit de votre souris.



Activez l'élément **Server Options**.



Double-cliquez sur le paramètre **DeviceLock Certificate** pour ouvrir la boîte de dialogue de configuration.



Renseignez le chemin d'accès de la clé privée dans le paramètre **Certificate Name** pour installer le certificat. Vous pouvez utiliser le bouton **...** pour sélectionner le fichier avec une clé privée.

Pour supprimer la clé privée, utilisez le bouton **Remove**.

Appuyez sur **OK** pour fermer la boîte de dialogue de configuration et appliquer les modifications.

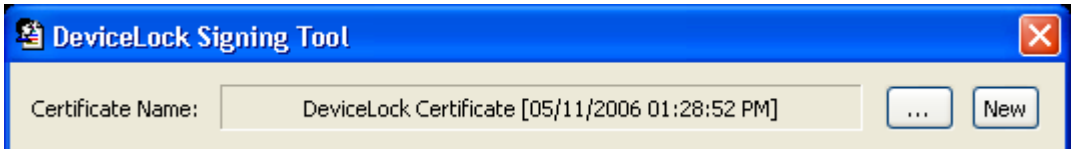
Pour plus de renseignements sur l'installation de la clé privée sur DeviceLock Enterprise Server et DeviceLock Content Security Server, veuillez vous reporter aux sections Installation de DeviceLock Enterprise Server et Installation de DeviceLock Content Security Server de ce manuel.

DeviceLock Signing Tool

Présentation

L'outil de signature de DeviceLock (DeviceLock Signing Tool) permet d'accorder aux utilisateurs un accès temporaire aux périphériques souhaités et de signer les fichiers XML contenant des paramètres DeviceLock Service exportés de DeviceLock Management Console ou de DeviceLock Group Policy Manager.

Pour exécuter l'outil de signature de DeviceLock, sélectionnez l'option **DeviceLock Signing Tool** dans le menu **File** de DeviceLock Enterprise Manager ou dans le menu contextuel de DeviceLock Management Console (l'extension MMC), de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor.



Commencez par charger le DeviceLock Certificate (la clé privée) correspondant.

Le DeviceLock Signing Tool doit utiliser la clé privée qui appartient au même certificat que la clé publique installée sur l'ordinateur de l'utilisateur.

Par défaut, le DeviceLock Signing Tool charge automatiquement le dernier certificat utilisé. Vous pouvez charger un autre certificat en appuyant sur le bouton **...** et en sélectionnant un fichier à l'aide de la clé privée.

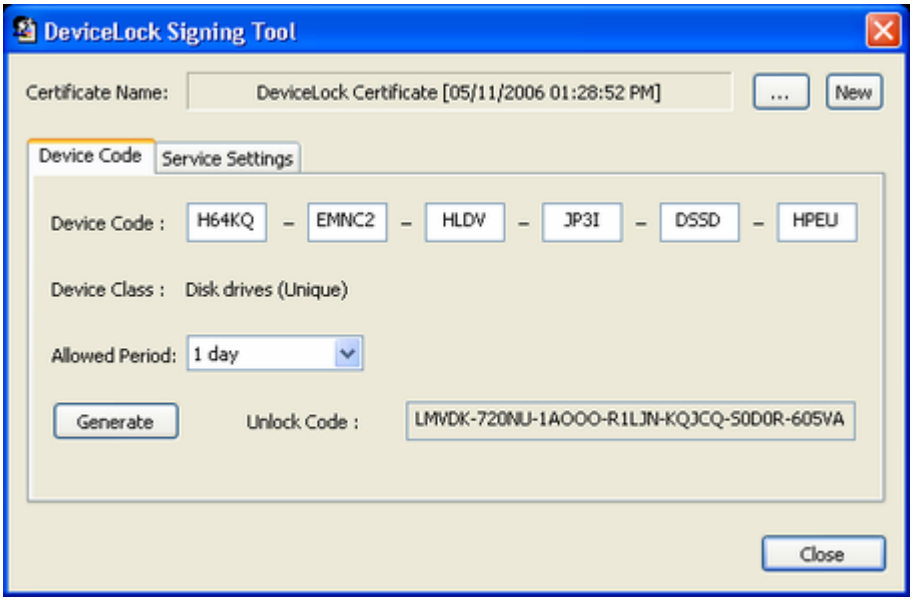
Pour générer le nouveau certificat, vous pouvez exécuter le Certificate Generation Tool directement à partir du DeviceLock Signing Tool. Pour ce faire, appuyez sur le bouton **New**. Néanmoins, n'oubliez pas que si vous générez un nouveau certificat et que vous essayez d'utiliser sa nouvelle clé privée dans le DeviceLock Signing Tool, vous devez aussi installer la clé publique correspondante sur l'ordinateur de l'utilisateur.

Puis, décidez de la marche à suivre: générer un code de déblocage ou signer un fichier XML contenant les paramètres de DeviceLock Service.

Device Code (Code de périphérique)

Pour accorder à l'utilisateur un accès temporaire à un périphérique, vous devez générer un **Unlock Code** (code de débloquage) à réception du **Device Code** (code de périphérique) de l'utilisateur en question.

Pour en savoir plus sur l'utilisation d'une temporary white list, consultez la section Temporary white list de ce manuel.



La génération d'un **Unlock Code** comporte quatre étapes simples :

1. Charger le DeviceLock Certificate correspondant (voir ci-dessus).
2. Saisir le **Device Code** que l'utilisateur vous communique.

   Dès que le bon **Device Code** est saisi, la catégorie du périphérique auquel l'utilisateur souhaite accéder apparaît dans le champ **Device Class**. La classe de périphérique permet de contrôler le type de périphérique que l'utilisateur envisage d'utiliser. Si, par exemple, un utilisateur dit à l'administrateur qu'il ou elle envisage d'utiliser un scanner USB tout en essayant en fait d'accéder à un lecteur flash USB, l'administrateur est en mesure de détecter l'anomalie.

   Un autre champ (placé entre parenthèses) indique également si le périphérique requis peut être autorisé en tant que périphérique individuel (**Unique**) ou ne peut l'être qu'en tant que modèle (**Model**), c'est-à-dire s'il possède ou non un numéro de série. Si vous autorisez le périphérique en tant que modèle, l'utilisateur dispose alors d'un accès à l'ensemble des périphériques de ce modèle. Pour plus d'informations sur le sujet, consultez la section USB Devices White List du présent manuel.

3. Choisir la période d'autorisation du périphérique considéré. Dans le champs **Allowed Period**, vous pouvez sélectionner différentes périodes prédéfinies: 5, 15, 30, 60 minutes, 5 heures, 1 ou 2 jours, 1 ou 2 semaines, un mois, jusqu'à la déconnexion de l'utilisateur ou le débranchement du périphérique.

   Si vous choisissez une période de temps fixe (p.ex. 10 minutes), l'utilisateur n'a accès au périphérique considéré que pendant la période en question. Dès la fin de la période d'autorisation, l'accès au périphérique est à nouveau refusé. Quel que soit le type d'action réalisée par l'utilisateur en fin de période – qu'il ou elle soit en train de copier des fichiers sur le disque USB ou d'imprimer un document sur l'imprimante USB par exemple, toutes les opérations seront interrompues.

   Pour permettre à l'utilisateur d'utiliser un périphérique donné sans limite de temps, choisissez **until unplug** dans **Allowed Period**. L'utilisateur aura alors accès au périphérique tant que celui-ci est branché sur le port. Dès que l'utilisateur débranche le périphérique en question, l'accès est à nouveau refusé.

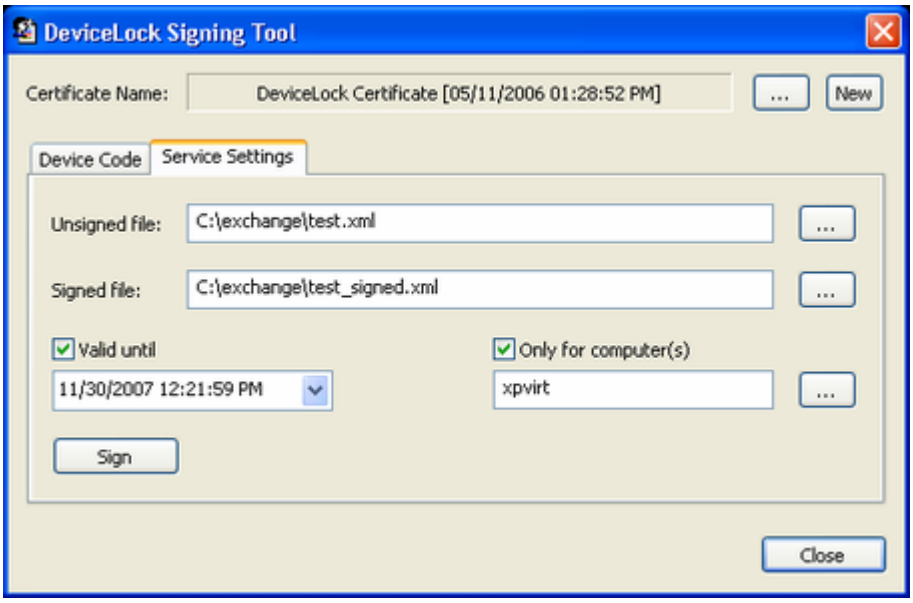
4. Appuyer sur le bouton **Generate** pour créer un **Unlock Code**. Communiquez ce code à l'utilisateur par voie téléphonique ou toute autre voie appropriée.

   Le processus de génération d'**Unlock Code** peut prendre un certain temps. En fonction de la vitesse de calcul de votre ordinateur, jusqu'à plusieurs secondes.

Service Settings (Paramètres de service)

Pour éviter toute modification intempestive, vous pouvez signer un fichier XML contenant des paramètres DeviceLock Service exportés de DeviceLock Management Console ou de DeviceLock Group Policy Manager ou créés à l'aide de DeviceLock Service Settings Editor.

Ce fichier peut ensuite être envoyé aux utilisateurs dont les ordinateurs ne sont pas en ligne et par conséquent hors de portée via les consoles de gestion.



La signature d'un fichier XML comporte six étapes simples:

1. Charger le DeviceLock Certificate correspondant (voir ci-dessus).
2. Charger les paramètres DeviceLock Service que vous devez signer dans le fichier.

   Le chemin complet vers ce fichier doit être spécifié dans le champ **Unsigned file**. Vous pouvez utiliser le bouton **...** pour sélectionner le fichier.

   Le fichier XML avec les paramètres de DeviceLock Service peut être créé à l'aide de l'option **Save Service Setting**s du menu contextuel de DeviceLock Management Console, de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor.

3. Spécifier le fichier resultant dans le champ **Signed file**. Vous pouvez utiliser le bouton **...** pour sélectionner le dossier dans lequel ce fichier sera créé.
4. Décider si le fichier résultant doit contenir des informations d'expiration ou pas.

Pour autoriser les utilisateurs à importer des paramètres de ce fichier sans limite de temps, décochez la case **Valid until**.

Si vous cochez la case **Valid until** et spécifiez la date et l'heure, les informations d'expiration s'inscrivent dans le fichier resultant et les utilisateurs peuvent importer les paramètres de ce fichier avant la date et l'heure indiquée.

Remarque: Ce paramètre n'affecte que les utilisateurs qui essaient d'importer des paramètres DeviceLock Service via l'applet **DeviceLock** du Panneau de configuration de Windows. Lorsqu'un fichier XML contenant des paramètres est chargé à l'aide de l'option **Load Service Settings** du menu contextuel dans DeviceLock Management Console ou DeviceLock Group Policy Manager, les informations d'expiration (s'il y en a) sont ignorées.

5. Décider si le fichier résultant peut être utilisé uniquement sur des ordinateurs particuliers ou non.

   Pour autoriser les utilisateurs à importer des paramètres de ce fichier sur n'importe quel ordinateur, décochez la case **Only for computer(s)**.

   Si vous cochez la case **Only for computer(s)** et spécifiez le nom de l'ordinateur, les utilisateurs ne pourront importer des paramètres de ce fichier que sur l'ordinateur indiqué. En utilisant le point-virgule (;) comme séparateur, vous pouvez spécifier plusieurs noms d'ordinateurs et ainsi utiliser le fichier résultant sur l'un ou l'autre des ordinateurs en question.

   Remarque: Vous ne pouvez pas utiliser l'adresse IP de l'ordinateur dans ce paramètre. Vous devez spécifier le nom de l'ordinateur exactement tel qu'il apparaît dans l'applet **Système** du **Panneau de configuration** de Windows.

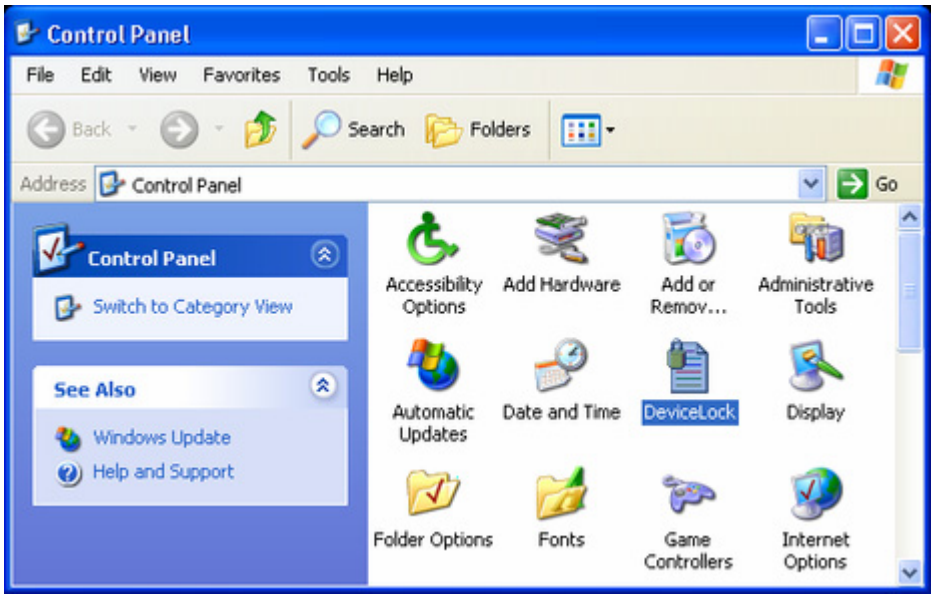
   Vous pouvez aussi charger une liste prédéfinie d'ordinateurs à partir du fichier de texte externe. Pour ouvrir un fichier externe, appuyez sur le bouton **...**. Ce fichier de texte doit contenir les noms de chacun des ordinateurs sur des lignes séparées.

   Remarque: Ce paramètre n'affecte que les utilisateurs qui essaient d'importer des paramètres DeviceLock Service via l'applet **DeviceLock** du Panneau de configuration de Windows. Lors du chargement d'un fichier XML avec paramètres à l'aide de l'option **Load Service Settings** du menu contextual dans DeviceLock Management Console ou DeviceLock Group Policy Manager, le nom de l'ordinateur est ignoré.

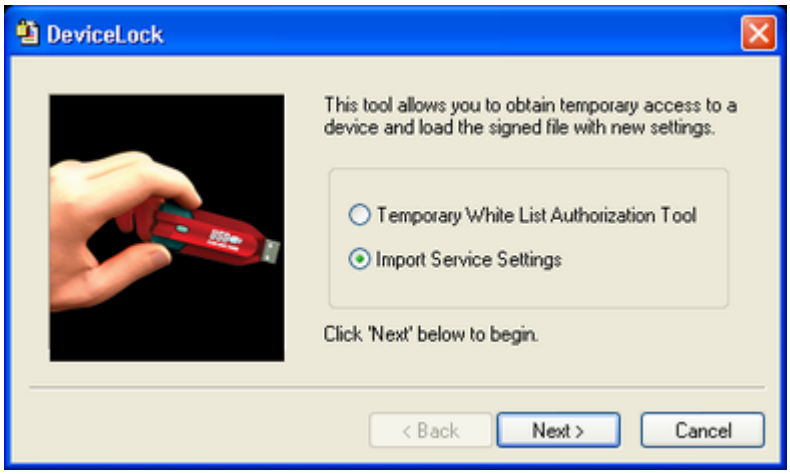
6. Appuyez sur le bouton **Sign** pour créer un fichier signé avec les paramètres de DeviceLock Service. Fournissez ce fichier à l'utilisateur comme bon vous semble.

   Le processus de signature de fichier peut prendre du temps. En fonction de la vitesse de calcul de votre ordinateur, jusqu'à plusieurs secondes.

Pour appliquer les paramètres de DeviceLock Service de ce fichier signé, l'utilisateur doit exécuter l'applet **DeviceLock** à partir du Control Panel et sélectionner l'option **Import Service Settings**.

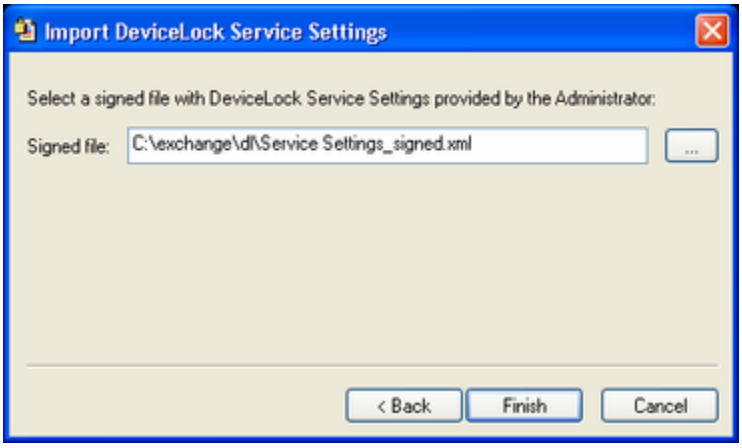


Remarque: Avec les versions XP et suivantes de Windows, l'utilisateur doit basculer en affichage classique du Control Panel pour pouvoir afficher l'ensemble des applets disponibles.


DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

Pour importer les paramètres de DeviceLock Service du fichier signé, l'utilisateur doit effectuer deux étapes simples:

1. Dans le champ **Signed file**, spécifier le chemin complet vers ce fichier signé. Utiliser le bouton **...** pour sélectionner le fichier.



2. Appuyer sur le bouton **Finish**. Si la signature numérique du fichier est valide, les nouveaux paramètres seront immédiatement appliqués à DeviceLock Service.

L'utilisateur peut également charger le fichier signé avec les paramètres DeviceLock Service à partir de la ligne de commande suivante:

DLTempAccess.cpl -s *<chemin vers le fichier signé>*

où *<chemin vers le fichier signé>* représente le chemin vers le fichier signé avec les paramètres DeviceLock Service. Par exemple:

DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"

Toutes les tentatives réussies de chargement des paramètres sont inscrites dans le journal, si la journalisation des changements est activée dans les Service Options.

DeviceLock Management Console

Présentation

DeviceLock Management Console est un module intégré au module Microsoft Management Console (MMC).

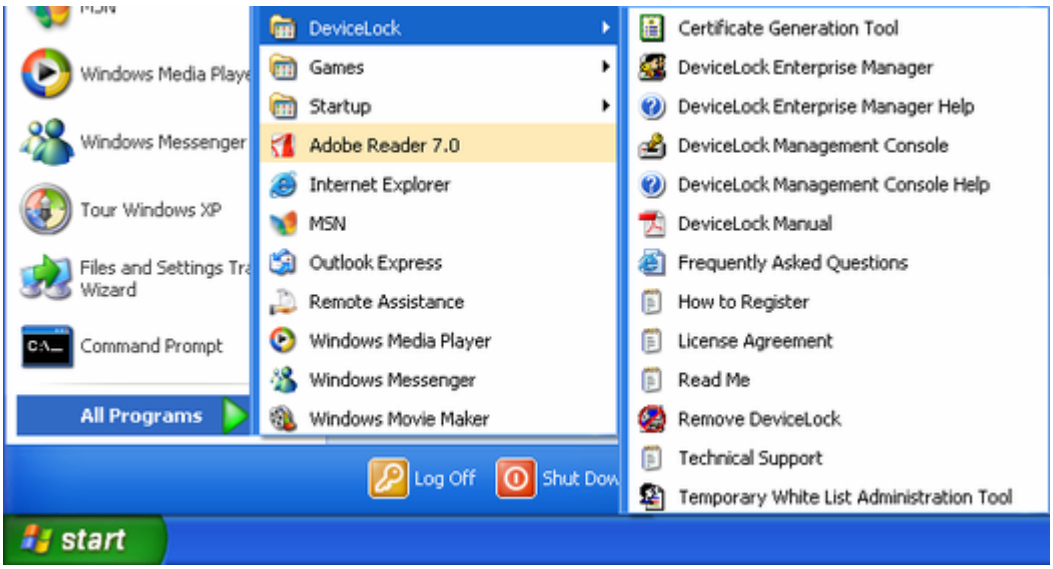
DeviceLock Management Console permet de voir et de modifier les autorisations et les règles d'audit, d'installer et mettre à jour DeviceLock Service et de visionner les rapports d'audit de chaque ordinateur.

DeviceLock Management Console sert aussi à visionner les journaux stockés sur DeviceLock Enterprise Server, à effectuer des recherches sur DeviceLock Content Security Server et à administrer ces serveurs.

DeviceLock Management Console doit être utilisé sur l'ordinateur à partir duquel l'administrateur gère DeviceLock Service et DeviceLock Enterprise Servers et DeviceLock Content Security Servers sur le réseau.

Pour des informations supplémentaires sur la manière d'installer DeviceLock Management Console, veuillez lire la section Installation des consoles de gestion de ce manuel.

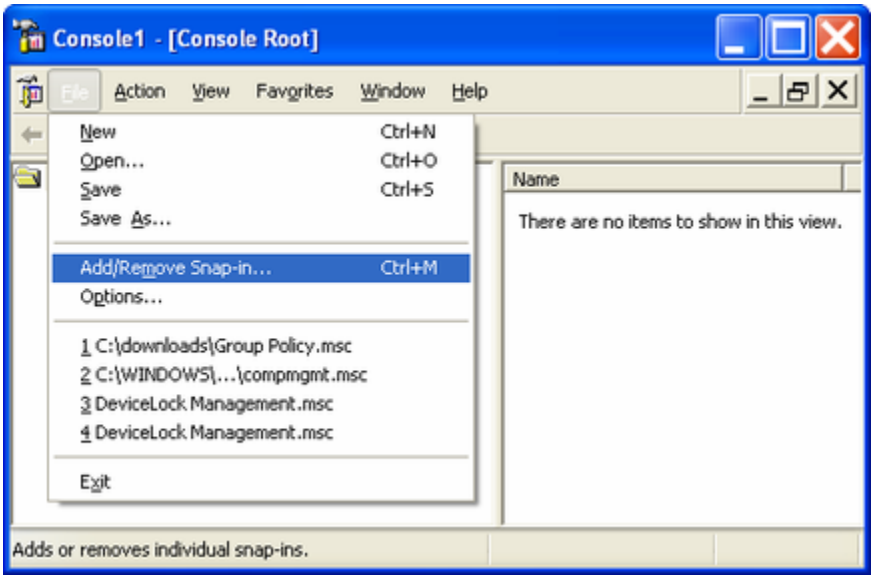
Pour exécuter DeviceLock Management Console, sélectionnez le raccourci approprié du menu **All Programs** disponible en cliquant sur le bouton **Start** de Windows.



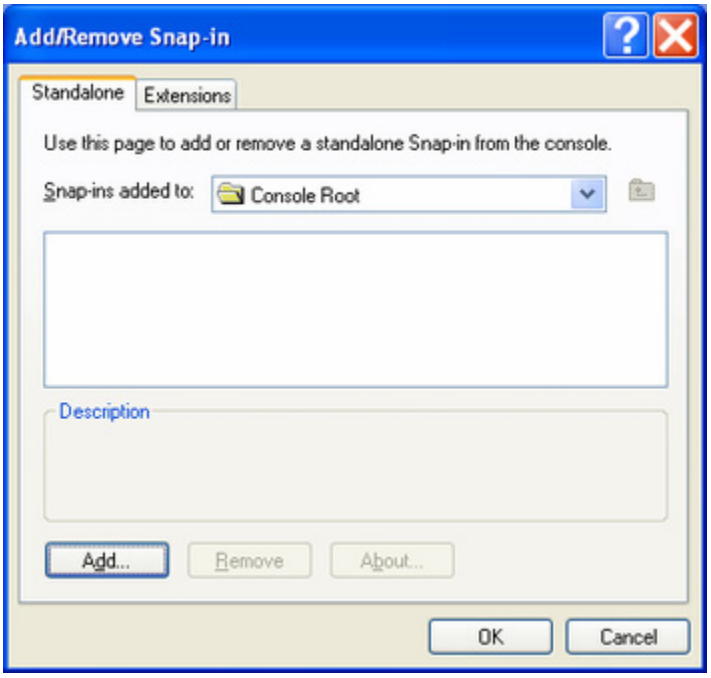
Il est également possible de démarrer MMC et d'ajouter le module intégré DeviceLock Management Console manuellement :

1. Lancez **mmc** à partir de la ligne de commande ou utilisez le menu **Run** pour exécuter cette commande.

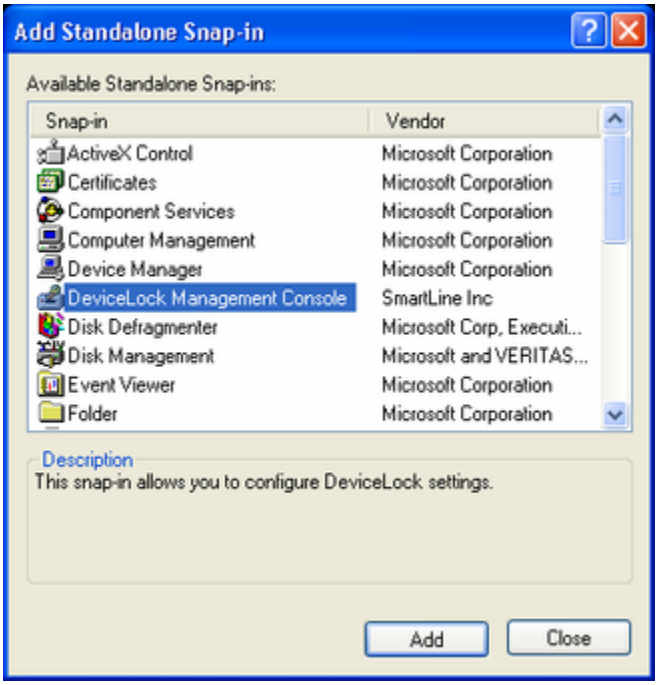
2. Ouvrez le menu **File**, puis cliquez sur **Add/Remove snap-in**.



3. Cliquez sur l'onglet **Standalone**, puis sur **Add**.

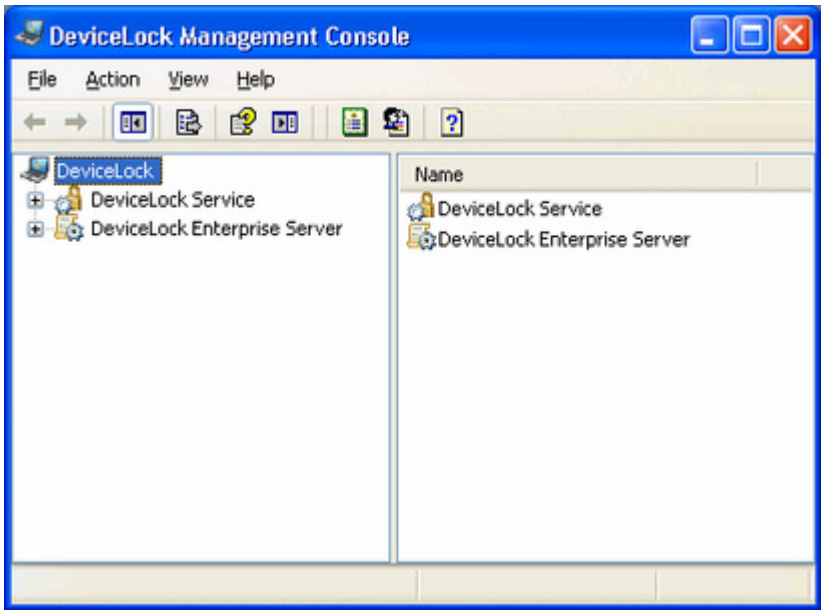


4. Choisissez **DeviceLock Management Console** dans la liste, puis cliquez sur **Add**.



Interface

DeviceLock Management Console possède une interface conviviale, facile à utiliser et standard, fournie par Microsoft Management Console (MMC). Lors de tout dialogue, vous pouvez appuyer sur la touche F1 pour accéder à une aide spécifique.



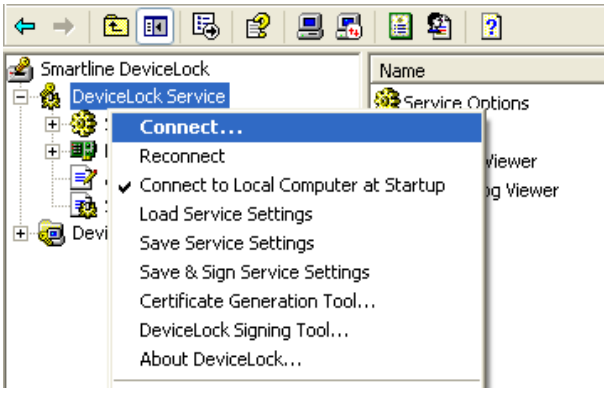
DeviceLock Management Console est constitué d'une fenêtre divisée en deux panneaux. Le panneau de gauche contient l'arborescence de console; le panneau de droite contient les détails correspondant. Lorsque vous sélectionnez un élément dans l'arborescence de console, les informations correspondantes s'affichent sur le panneau de détails.

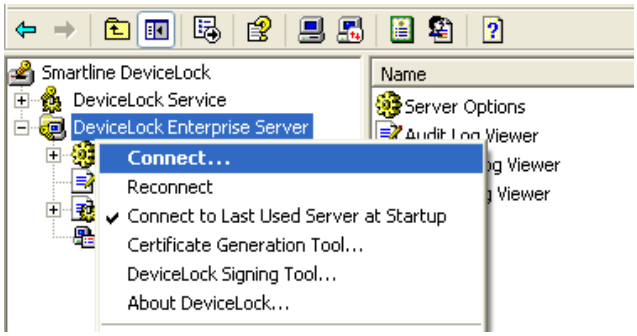
DeviceLock Management Console est composé de trois parties indépendantes:

1. **DeviceLock Service** – qui permet de se connecter et d'administrer les DeviceLock Services en cours d'exécution sur les ordinateurs locaux et distants.
2. **DeviceLock Enterprise Server** – qui permet de se connecter et d'administrer les DeviceLock Enterprise Servers en cours d'exécution sur les ordinateurs locaux et distants.
3. **DeviceLock Content Security Server** – qui permet de se connecter et d'administrer les DeviceLock Content Security Servers en cours d'exécution sur les ordinateurs locaux et distants.

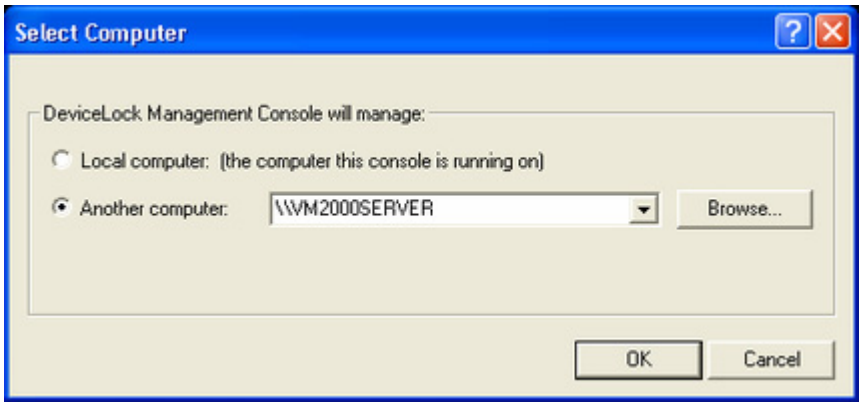
Connexion aux ordinateurs

Vous devez tout d'abord vous connecter à l'ordinateur qui exécute DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server. Utilisez l'option **Connect** du menu contextuel ou l'icône appropriée de la barre d'outils.





Vous pouvez vous connecter simultanément à DeviceLock Service, à DeviceLock Enterprise Server et à DeviceLock Content Security Server, même si ces trois programmes s'exécutent sur des ordinateurs distincts.



Spécifiez le nom ou l'adresse IP de l'ordinateur auquel vous voulez vous connecter dans le paramètre **Another Computer**. Pour naviguer vers les ordinateurs disponibles sur votre réseau, utilisez le bouton **Browse**.

Pour connecter DeviceLock Management Console à l'ordinateur sur lequel DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server a été configuré à l'aide d'un port fixe, vous devez spécifier le numéro de ce port entre crochets à côté du nom de l'ordinateur. Ex: *ordinateur_nom[numéro du port]*.

Pour vous connecter à l'ordinateur local, choisissez l'option **Local computer**.

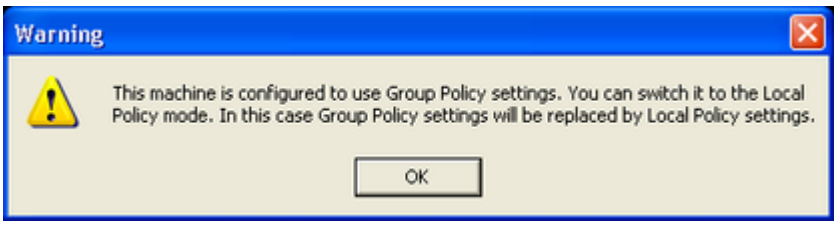
Cliquez sur **OK** pour vous connecter à l'ordinateur en question.

Remarque: Vérifiez que l'ordinateur distant que vous avez sélectionné est accessible à partir de l'ordinateur qui exécute DeviceLock Management Console. L'ordinateur distant doit utiliser un système d'exploitation compatible avec DeviceLock (Windows NT4.0 SP6 ou plus récent). Le protocole TCP/IP doit être activé. Le pare-feu éventuel (y compris le pare-feu Windows intégré) doit être correctement configuré afin de permettre la connexion avec DeviceLock Service, DeviceLock Enterprise Server et/ou DeviceLock Content Security Server.

DeviceLock Service s'ajoute automatiquement à la liste des exceptions du pare-feu Windows.

Lorsque vous essayez de vous connecter à un ordinateur sur lequel DeviceLock Service n'est pas installé ou n'est pas à jour, DeviceLock Management Console vous propose de l'installer ou de le mettre à jour. Pour plus d'informations sur le déploiement de services à distance, veuillez lire le chapitre Installation à distance via DeviceLock Management Console de ce manuel.

Vous recevez le message d'avertissement lorsque vous vous connectez à DeviceLock Service configuré en mode Politique de groupe.


Warning
This machine is configured to use Group Policy settings. You can switch it to the Local Policy mode. In this case Group Policy settings will be replaced by Local Policy settings.
OK

Si vous changez un paramètre quelconque à l'aide de DeviceLock Management Console, ce paramètre retrouvera son état original (défini dans GPO) lors de la prochaine mise à jour de politique de groupe. Pour plus d'informations, veuillez lire le chapitre Service Options de ce manuel.

Si vous essayez de vous connecter à DeviceLock Enterprise Server ou DeviceLock Content Security Server sur un ordinateur ou celui-ci n'est pas installé ou est arrêté, vous obtenez une erreur de connexion.

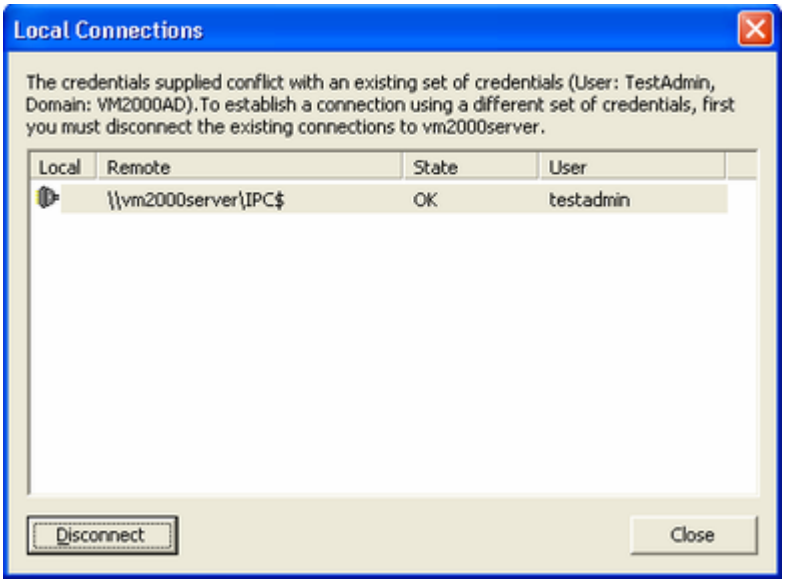
DeviceLock Enterprise Server et DeviceLock Content Security Server doivent être installés et lancés pour pouvoir y connecter DeviceLock Management Console. Pour plus de détails sur le déploiement des serveurs, veuillez vous reporter aux sections Installation de DeviceLock Enterprise Server et Installation de DeviceLock Content Security Server de ce manuel.

Si vous ne disposez pas de privilèges d'administration sur l'ordinateur sélectionné, DeviceLock Management Console vous propose de vous y connecter avec le compte d'un autre utilisateur.

Dans le paramètre **Connect As**, vous pouvez renseigner un compte utilisateur avec les privilèges d'administration nécessaires. Ce compte doit aussi figurer sur la liste des administrateurs DeviceLock, au cas où cette fonction de protection des administrateurs a été activée pour DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server.

Si, une fois connecté à un ordinateur (comportant un disque réseau lié, une ressource réseau partagée, etc.) via un compte qui n'a pas accès à DeviceLock Service, à DeviceLock Enterprise Server ou à DeviceLock Content Security Server, vous essayez d'utiliser un autre compte d'utilisateur dans DeviceLock Management Console, un «conflit d'accréditations» risque de se produire. Pour éviter ce genre de conflit, supprimez d'abord votre connexion existante.

Lorsque DeviceLock Management Console détecte un conflit d'accréditations, le système affiche la liste des connexions existantes sur votre ordinateur local et vous propose d'en supprimer quelques-unes.



Sélectionnez toutes les connexions de l'ordinateur auquel vous voulez vous connecter et appuyez sur **Disconnect**.

Appuyez sur **Close**, puis renouvelez votre tentative de connexion à cet ordinateur.

Remarque: Il peut arriver que la connexion existante ne puisse pas être supprimée, ce qui vous empêche d'utiliser un compte utilisateur différent dans DeviceLock Management Console. Dans ce cas, il faut exécuter DeviceLock Management Console avec un compte utilisateur qui dispose de suffisamment de privilèges pour exécuter DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server, ou n'est pas connecté avec l'ordinateur en question. Vous pouvez utiliser la fonction Run as (exécutez RUNAS dans la ligne de commande) de Windows 2000 et versions ultérieures, pour exécuter DeviceLock Management Console avec un autre compte.

Erreurs de connexion possibles

Lorsque vous essayez de vous connecter à un ordinateur exécutant DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server, les erreurs suivantes peuvent se produire:

- **(1722) The RPC server is unavailable**: Vous essayez de vous connecter à un ordinateur inexistant (nom ou adresse IP erroné) ou qui n'est pas accessible. Vérifiez le nom d'ordinateur que vous avez spécifié. Essayez de faire un Ping vers cet ordinateur en utilisant son nom et son adresse IP, et connectez-vous y à l'aide d'un outil standard d'administration Windows (tel que Computer Management, Services, etc.). Assurez-vous que l'ordinateur en question utilise un système d'exploitation compatible avec DeviceLock (Windows NT 4.0 et plus récent).

  Il se peut également qu'un pare-feu bloque l'accès à cet ordinateur. Vous devez configurer votre pare-feu pour permettre l'accès aux ports nécessaires pour DeviceLock. Vous pouvez aussi ordonner à DeviceLock d'utiliser un port TCP fixe, ce qui simplifie la configuration du pare-feu. Par défaut, DeviceLock Service, DeviceLock Enterprise Server et DeviceLock Content Security Server utilisent les ports 9132 et

9133 et 9134 dans la suite. Pour plus d'informations, veuillez vous reporter à la section FAQ de notre site Web. Veuillez aussi noter que DeviceLock Service s'ajoute automatiquement à la liste des exceptions du pare-feu Windows.

- **(1753) There are no more endpoints available from the endpoint mapper**: Vous essayez de vous connecter à un ordinateur sur lequel DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server n'est pas disponible. Vérifiez tout d'abord que DeviceLock Service, DeviceLock Enterprise Server ou DeviceLock Content Security Server est installé et activé sur l'ordinateur distant.

  Peut-être cet ordinateur vient-il juste d'être mis en route, et Windows est encore en train d'initialiser ses services. Le service Remote Procedure Call (RPC) n'a peut-être pas encore été démarré.

  Il se peut également qu'un pare-feu bloque l'accès à DeviceLock Service, à DeviceLock Enterprise Server ou à DeviceLock Content Security Server. Pour plus d'informations, veuillez consulter la description de l'erreur 1722 ci-dessus.

  Pour remédier aux erreurs de RPC Endpoint Mapper, veuillez lire l'article Microsoft suivant: http://support.microsoft.com/kb/839880/fr

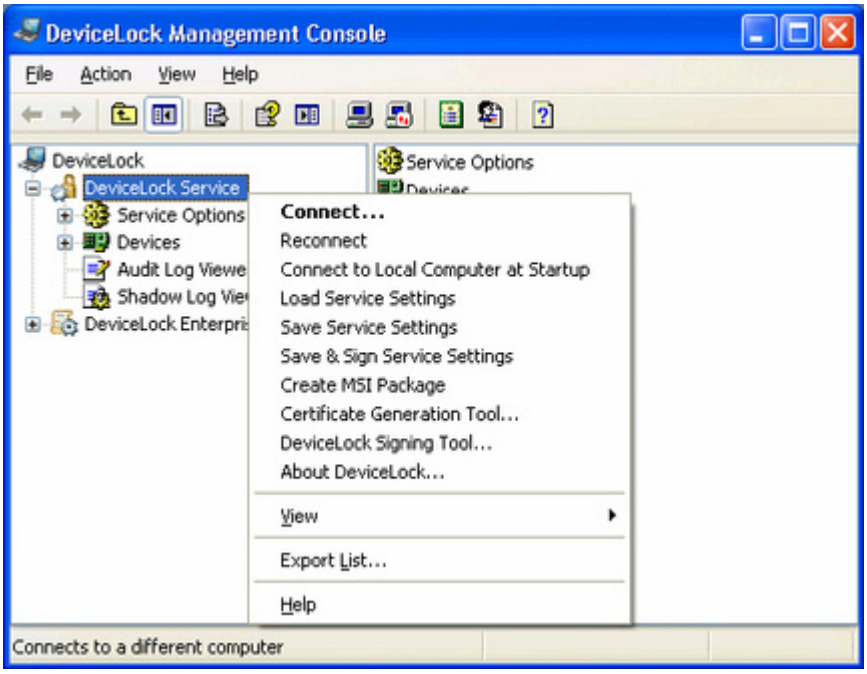
- **(5) Access is denied**: vous manquez de privilèges sur l'ordinateur distant. Assurez-vous que DeviceLock Management Console essaye de se connecter à l'ordinateur distant en tant qu'utilisateur disposant de privilèges d'administrateur local sur cet ordinateur.

  Vous risquez également de devoir exécuter DeviceLock Management Console sous un autre compte d'utilisateur, capable de s'identifier sur la machine distante en tant administrateur local.

- **(7045) You must have administrative privileges to perform this operation**: vous n'avez pas les privilèges nécessaires pour accéder à DeviceLock Service, à DeviceLock Enterprise Server ou à DeviceLock Content Security Server parce que l'utilisateur n'appartient pas à la liste des administrateurs DeviceLock. Assurez-vous que DeviceLock Management Console essaie de se connecter à l'ordinateur distant en tant qu'utilisateur appartenant à la liste des administrateurs DeviceLock de cet ordinateur.

Administration de DeviceLock Service

Développez l'élément **DeviceLock Service** afin d'accéder à tous les paramètres de configuration et fonctionnalités du service.



Un menu contextuel est disponible: cliquez droit sur l'élément **DeviceLock Service** en question:

- **Connect**: permet la connexion à tout ordinateur spécifié. Pour plus d'informations, veuillez lire le chapitre Connexion aux ordinateurs de ce manuel.
- **Reconnect**: renouvelle la connexion à l'ordinateur actuellement connecté.
- **Connect to Local Computer at Startup**: cochez cette option pour ordonner à DeviceLock Management Console de se connecter automatiquement à l'ordinateur local à chaque démarrage.
- **Load Service Settings**: charge les paramètres enregistrés précédemment à partir du fichier XML et les applique au DeviceLock Service actuellement connecté. Vous devez sélectionner le fichier créé soit par DeviceLock Service Settings Editor, par DeviceLock Management Console ou par DeviceLock Group Policy Manager. Etant donné que la signature n'est pas validée à ce stade, il peut s'agir d'un fichier signé ou non signé.
- **Save Service Settings**: exporte tous les paramètres du DeviceLock Service actuellement connecté à un fichier XML externe. Ce fichier peut ensuite être modifié à l'aide de DeviceLock Service Settings Editor et chargé via DeviceLock Management Console et/ou DeviceLock Group Policy Manager. Ce fichier peut aussi être envoyé aux utilisateurs dont les ordinateurs ne sont pas en ligne et par conséquent hors de portée via les consoles de gestion. Pour éviter toute modification non autorisée, le fichier doit être signé avec le DeviceLock Certificate (la clé privée) à l'aide du DeviceLock Signing Tool.
- **Save & Sign Service Settings**: exporte tous les paramètres du DeviceLock Service actuellement connecté dans un fichier XML externe et le signe automatiquement avec le DeviceLock Certificate (la clé privée) le plus récent. Cet élément de menu est

désactivé lorsqu'aucune clé privée n'est encore chargée dans le DeviceLock Signing Tool.

- **Certificate Generation Tool**: lance l'outil spécial qui permet de générer des DeviceLock Certificates. Pour plus d'informations, veuillez lire le chapitre Création de DeviceLock Certificates de ce manuel.
- **Create MSI Package**: crée le progiciel Microsoft Software Installer (MSI) personnalisé avec des paramètres du DeviceLock Service connecté au moment considéré.

  Dans une première étape, vous devez sélectionner le progiciel MSI source avec DeviceLock Service. Vous pouvez utiliser des progiciels MSI livrés avec DeviceLock (comme DeviceLock Service.msi et DeviceLock Service x64.msi).

  Puis vous devez préciser le nom du progiciel MSI résultant (cible) qui sera généré en fonction du progiciel MSI source (indiqué dans la première étape) et des paramètres du DeviceLock Service connecté au moment considéré.

  Ensuite, ce progiciel MSI personnalisé peut être utilisé pour déployer des instances de DeviceLock Service dans l'ensemble du réseau avec des politiques prédéfinies. Pour plus de détails sur le déploiement de DeviceLock Service à l'aide de MSI, veuillez vous reporter au chapitre Installation via Group Policy de ce manuel.

  Remarque : Si vous utilisez un progiciel MSI personnalisé avec les paramètres définis par DeviceLock Service afin de déployer DeviceLock Service en utilisant la politique de groupe, ces paramètres ne sont pas appliqués aux ordinateurs clients si l'une des conditions suivantes est remplie:

  - La sécurité par défaut est désactivée sur l'exécution des DeviceLock Service distants.

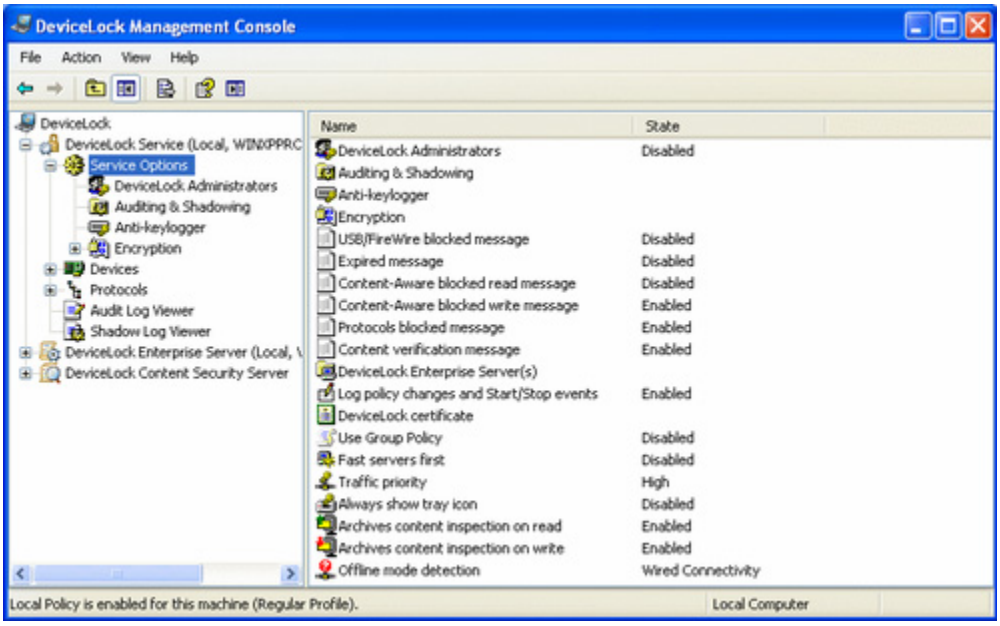
  - La politique de groupe GPO appliquée aux ordinateurs clients a le paramètre **Override Local Policy** activé.

  Veuillez noter que l'élément de menu **Create MSI Package** est désactivé lorsqu'aucun Microsoft Windows Installer (version 1.0 ou suivante) n'est installé sur l'ordinateur local.

- **DeviceLock Signing Tool**: exécute l'outil spécial qui permet d'accorder aux utilisateurs un accès temporaire aux périphériques demandés et de signer les fichiers XML avec les paramètres de DeviceLock Service. Pour plus d'informations, veuillez vous reporter à la section DeviceLock Signing Tool de ce manuel.
- **About DeviceLock**: ouvre une boîte de dialogue contenant des informations sur la version de DeviceLock employée et sur vos licences.

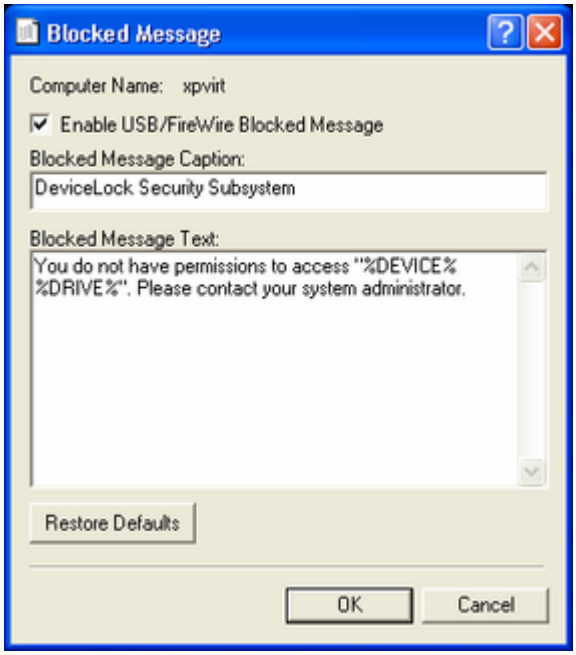
Service Options (Options de service)

Ces paramètres supplémentaires permettent d'améliorer la configuration de DeviceLock Service. Utilisez le menu contextuel accessible par simple clic droit de votre souris sur chaque paramètre.



USB/FireWire blocked message (Message bloqué USB/FireWire)

Vous pouvez personnaliser le message affiché à l'attention des utilisateurs lorsque l'accès à un périphérique USB ou FireWire est refusé au niveau de l'interface (USB ou FireWire) ou au niveau typologique (lecteur amovible, CD/DVD, etc.).



Pour permettre l'affichage du message personnalisé, cochez la case **Enable USB/FireWire Blocked Message**.

Vous pouvez aussi définir d'autres paramètres, notamment:

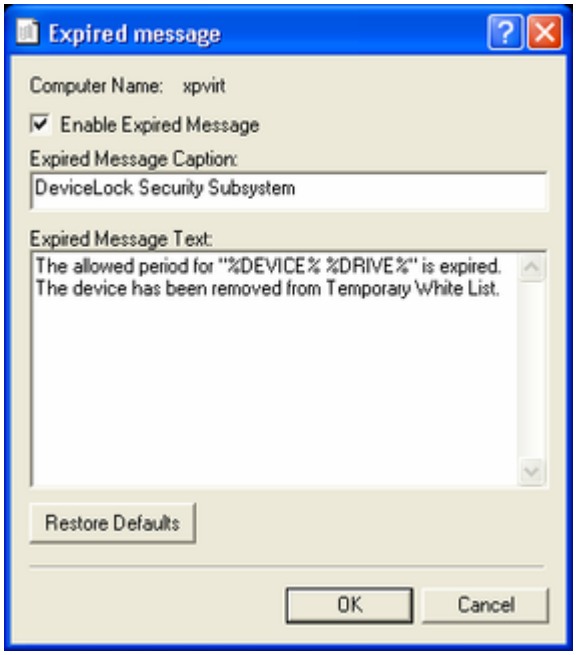
- **Blocked Message Caption**: le texte sera affiché sous forme de titre. Vous pouvez utiliser trois variables dynamiques prédéfinies au sein du texte:
  - **%TYPE%**: insère le nom du port (port USB, port FireWire) sur lequel le périphérique bloqué est connecté.
  - **%DEVICE%**: insère le nom du périphérique (p.ex. Périphérique de stockage de masse USB) reçu du système.
  - **%DRIVE%**: insère la lettre de lecteur du périphérique de stockage (p.ex. F:). Si le périphérique n'a pas de lettre, cette variable insert une chaîne vide.

  Avec ces variables dynamiques, vous pouvez créer d'autres messages d'information à l'intention des utilisateurs.

- **Blocked Message Text**: le texte principal du message. Vous pouvez utiliser les variables dynamiques prédéfinies décrites ci-dessus au sein du texte.

Expired message (Message expiré)

Vous pouvez définir un message personnalisé que les utilisateurs verront lorsque le temps imparti pour les dispositifs sur temporary white list est écoulé et une fois ces dispositifs rejetés de la Temporary white list.



Pour permettre l'affichage du message personnalisé, cochez la case **Enable Expired Message**.

Vous pouvez aussi définir d'autres paramètres, notamment:

- **Expired Message Caption**: le texte sera affiché sous forme de titre. Vous pouvez utiliser deux variables dynamiques prédéfinies au sein du texte:

- **%DEVICE%**: insère le nom du périphérique (p.ex. Périphérique de stockage de masse USB) reçu du système.
- **%DRIVE%**: insère la lettre de lecteur du périphérique de stockage (p.ex. F:). Si le périphérique n'a pas de lettre, cette variable insert une chaîne vide.

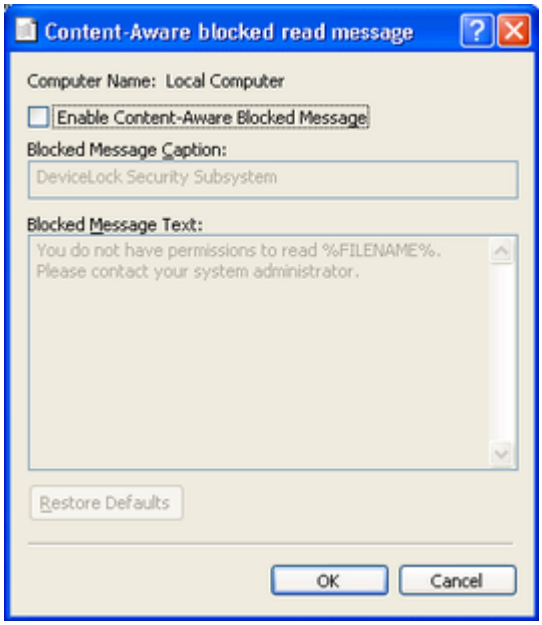
Avec ces variables dynamiques, vous pouvez créer d'autres messages d'information à l'intention des utilisateurs.

- **Expired Message Text**: le texte principal du message. Vous pouvez utiliser les variables dynamiques prédéfinies décrites ci-dessus au sein du texte.

Content-Aware Blocked Read Message

Vous pouvez définir un Content-Aware blocked read message (message de lecture bloquée contextuel) à afficher aux utilisateurs lorsqu'ils tentent de lire un fichier auquel ils n'ont pas accès. Cette info-bulle s'affiche dans la zone de notification de la barre des tâches sur les postes client. Par défaut, DeviceLock n'affiche pas le message de lecture bloquée contextuel.

Pour activer ou désactiver le message de lecture bloquée contextuel, cliquez droit sur **Content-Aware blocked read message**, puis cliquez sur **Properties** ou double-cliquez sur **Content-Aware blocked read message**.



Dans la boîte de dialogue **Content-Aware blocked read message**, procédez comme suit:

UTILISEZ CECI	POUR FAIRE CELA
Enable Content-Aware Blocked Message	Activer ou désactiver l'affichage du message Content-Aware blocked read. Cocher la case **Enable Content-Aware Blocked Message** pour activer l'affichage du message.

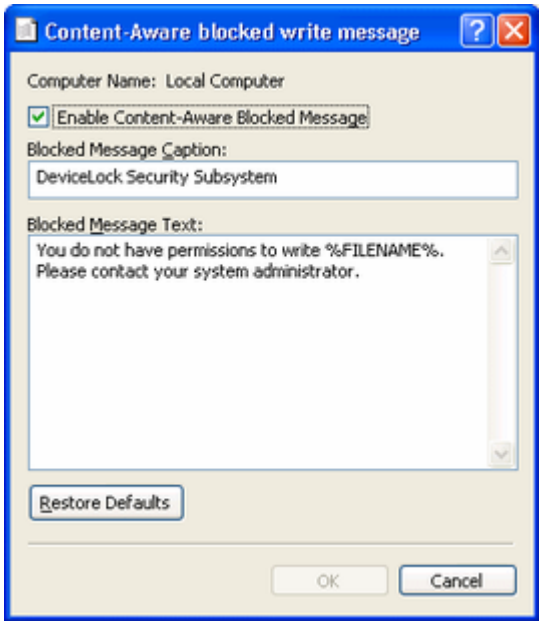
UTILISEZ CECI	POUR FAIRE CELA
	Décocher la case **Enable Content-Aware Blocked Message** pour désactiver l'affichage du message.
Blocked Message Caption	Définir le texte à afficher dans la barre de titre de la bulle de message. Par défaut, le titre de message de blocage est le suivant: **DeviceLock Security Subsystem**
Blocked Message Text	Définir le texte à afficher dans la bulle de message. Par défaut, le texte de message de blocage du message de lecture bloquée en fonction du contenu est le suivant: **You do not have permissions to read %FILENAME%. Please contact your system administrator.** où **%FILENAME% -** est le chemin et le nom de fichier du fichier à insérer.
Restore Defaults	Restaurer les paramètres par défaut.

Pour une description détaillée des règles contextuelles, consultez les chapitres «Règles contextuelles pour les périphériques (Regular Profile)» et «Règles contextuelles pour les protocoles (Regular Profile).»

Content-Aware Blocked Write Message

Vous pouvez définir un Content-Aware blocked write message (message d'écriture bloquée contextuel) à afficher aux utilisateurs lorsqu'ils tentent d'écrire dans un fichier auquel ils n'ont pas accès. Cette info-bulle s'affiche dans la zone de notification de la barre des tâches sur les postes client. Par défaut, DeviceLock n'affiche pas le message d'écriture bloquée contextuel.

Pour activer ou désactiver le message d'écriture bloquée contextuel, cliquez droit sur **Content-Aware blocked write message**, puis cliquez sur **Properties** ou double-cliquez sur **Content-Aware blocked write message**.



Dans la boîte de dialogue **Content-Aware blocked write message**, procédez comme suit:

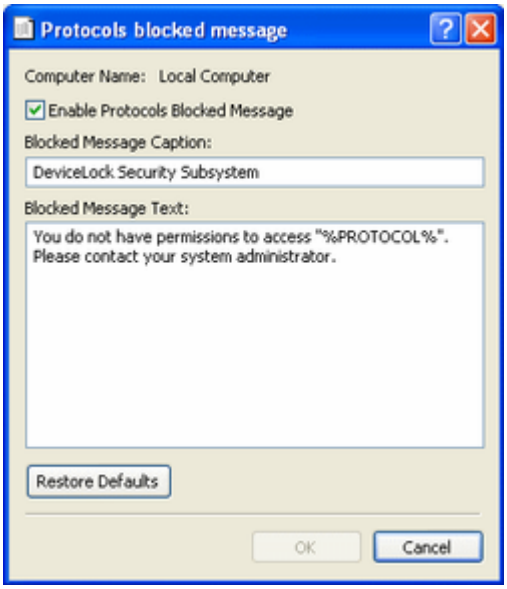
UTILISEZ CECI	POUR FAIRE CELA
Enable Content-Aware Blocked Message	Activer ou désactiver l'affichage du message Content-Aware blocked write. Cocher la case **Enable Content-Aware Blocked Message** pour activer l'affichage du message. Décocher la case **Enable Content-Aware Blocked Message** pour désactiver l'affichage du message.
Blocked Message Caption	Définir le texte à afficher dans la barre de titre de la bulle de message. Par défaut, le titre de message de blocage est le suivant: **DeviceLock Security Subsystem**
Blocked Message Text	Définir le texte à afficher dans la bulle de message. Par défaut, le texte de message de blocage du message d'écriture bloquée en fonction du contenu est le suivant : **You do not have permissions to write %FILENAME%. Please contact your system administrator.** où %FILENAME% - est le chemin et le nom de fichier du fichier à insérer.
Restore Defaults	Restaurer les paramètres par défaut.

Pour une description détaillée des règles contextuelles, consultez les chapitres «Règles contextuelles pour les périphériques (Regular Profile)» et «Règles contextuelles pour les protocoles (Regular Profile).»

Protocols blocked message

Vous pouvez définir un Protocols blocked message (message en cas de blocage de protocoles) à afficher aux utilisateurs lorsqu'ils essaient d'accéder à un protocole auquel ils n'ont pas accès. Cette info-bulle s'affiche dans la zone de notification de la barre des tâches sur les postes client.

Pour activer ou désactiver un Protocols blocked message, faites un clic droit sur **Protocols blocked message**, puis cliquez sur **Properties**, ou alors double-cliquez sur **Protocols blocked message**.



Dans la boîte de dialogue **Protocols blocked message**, procédez comme suit:

UTILISEZ CETTE OPTION	POUR FAIRE CECI
Enable Protocols Blocked Message	Activer ou désactiver l'affichage des Protocols blocked message. Cochez la case **Enable Protocols Blocked Message** pour activer l'affichage du message. Décochez la case **Enable Protocols Blocked Message** pour désactiver l'affichage du message.
Blocked Message Caption	Définir le texte à afficher dans la barre de titre de la bulle de message. Le texte par défaut du Block Message Caption est le suivant: **DeviceLock Security Subsystem**
Blocked Message Text	Définir le texte à afficher dans la bulle de message. Le texte par défaut du Blocked Message Text est le suivant: **You do not have permissions to access %PROTOCOL%. Please contact your system administrator**. **%PROTOCOL%** désignant le protocole faisant l'objet d'une restriction

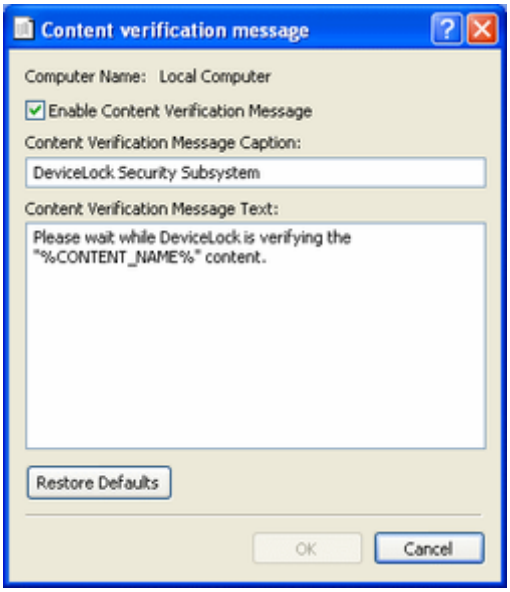
UTILISEZ CETTE OPTION	POUR FAIRE CECI
	d'accès.
Restore Defaults	Restaurer les paramètres par défaut.

Pour une description détaillée de la fonction Protocols, consultez le chapitre «Protocoles (Regular Profile).»

Content verification message

La vérification du contenu des fichiers copiés vers des périphériques ou transmis sur le réseau peut prendre un certain temps. Vous pouvez définir un «Content verification message» à afficher aux utilisateurs lorsque la vérification de contenu est en cours. Ce message s'affiche 20 secondes après le début de la vérification du contenu du fichier par DeviceLock Service.

Pour activer ou désactiver un Content verification message, faites un clic droit sur **Content verification message**, puis cliquez sur **Properties**, ou alors double-cliquez sur **Content verification message**.



Dans la boîte de dialogue **Content verification message**, procédez comme suit:

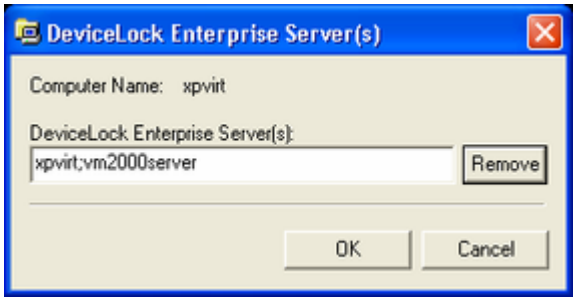
UTILISEZ CETTE OPTION	POUR FAIRE CECI
Enable Content Verification Message	Activer ou désactiver l'affichage des Content verification message. Cochez la case **Enable Content Verification Message** pour activer l'affichage du message.

UTILISEZ CETTE OPTION	POUR FAIRE CECI
	Décochez la case **Enable Content Verification Message** pour désactiver l'affichage du message.
Content Verification Message Caption	Définir le texte à afficher dans la barre de titre de la boîte de message. Le texte par défaut du Content Verification Message Caption est le suivant: **DeviceLock Security Subsystem**
Content Verification Message Text	Définir le texte à afficher dans la boîte de message. Le texte par défaut du Content Verification Message Text est le suivant: **Please wait while DeviceLock is verifying the %CONTENT_NAME% content. (Veuillez patienter pendant que DeviceLock vérifie le contenu de %CONTENT_NAME%.)** **%CONTENT_NAME%** désignant le fichier ou le protocole faisant l'objet d'une restriction d'accès. Le nom du fichier est inséré lorsque DeviceLock vérifie le contenu du fichier copié vers un périphérique. Le nom du protocole est inséré lorsque DeviceLock vérifie le contenu des données transmis sur le réseau.
Restore Defaults	Restaurer les paramètres par défaut.

Pour une description détaillée des règles contextuelles, consultez les chapitres «Règles contextuelles pour les périphériques (Regular Profile)» et «Règles contextuelles pour les protocoles (Regular Profile).»

DeviceLock Enterprise Server(s)

Si vous voulez que DeviceLock Service envoie ses journaux à DeviceLock Enterprise Server, indiquez le nom ou l'adresse IP de l'ordinateur du serveur considéré.



Grâce au point-virgule (;) utilisé comme séparateur, vous pouvez spécifier plusieurs DeviceLock Enterprise Server pour répartir uniformément la charge du réseau. Au démarrage, DeviceLock Service choisit un serveur pour envoyer ses rapports. Si le serveur choisi n'est pas disponible, DeviceLock Service en essaie un autre dans la liste.

Attention: DeviceLock Enterprise Server doit être installé dans les règles de l'art et accessible à DeviceLock Service, faute de quoi les rapports ne seront pas stockés dans la base de données centralisée. Pour plus de renseignements sur l'installation du DeviceLock

Enterprise Server, veuillez vous reporter à la section Installation de DeviceLock Enterprise Server de ce manuel.

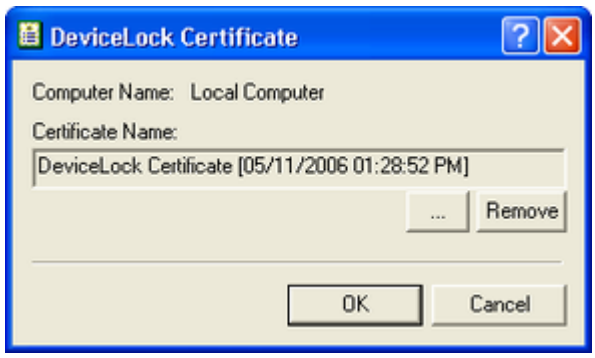
Log Policy changes and Start/Stop events (Changements de politique de journal et Démarrages/Arrêts)

Vous pouvez activer l'audit des modifications dans la configuration de DeviceLock Service et indiquer l'heure à laquelle DeviceLock Service démarre et s'interrompt. Il est possible de répertorier les modifications d'autorisations, de règles d'audit, de listes blanches et d'autres paramètres.

Pour permettre cet audit, cochez la case **Log Policy Changes and Start/Stop Events**.

DeviceLock certificate (Certificat DeviceLock)

Utilisez ce paramètre pour installer ou supprimer un DeviceLock Certificate.



Renseignez le chemin d'accès de la clé publique dans le paramètre **Certificate Name** pour installer le certificat. Vous pouvez utiliser le bouton **...** pour sélectionner le fichier avec la clé publique. Pour supprimer la clé publique, utilisez le bouton **Remove**.

Pour plus de détails sur DeviceLock Certificate, veuillez vous référer au chapitre DeviceLock Certificates de ce manuel.

Use Group Policy (Utilisation de la politique de groupe)

Si DeviceLock Service est configuré pour travailler avec les politiques de groupe (GPOs) dans un domaine Active Directory, vous pouvez contrôler le mode Effective Policy (Group Policy ou Local Policy).

Pour activer le mode Group Policy de ce DeviceLock Service, activez le paramètre **Use Group Policy**. Dans ce mode, toutes les configurations mises en place via DeviceLock Management Console et DeviceLock Enterprise Manager sont remplacées par la configuration des politiques de groupe.

Pour activer le mode Local Policy pour ce DeviceLock Service, activez le paramètre **Use Group Policy**. Dans ce mode, toute configuration mise en place par DeviceLock Manager est prioritaire sur la configuration des politiques de groupe et la remplace.

Si DeviceLock n'est pas configuré pour travailler avec les politiques de groupe, le paramètre **Use Group Policy** est décoché et désactivé.

Si le paramètre **Use Group Policy** est activé mais impossible à modifier, c'est que le mode Group Policy est toujours prioritaire (le paramètre **Override Local Policy** a été activé dans DeviceLock Group Policy Manager) et le mode Local Policy ne peut pas être activé pour ce DeviceLock Service. Pour plus d'informations, veuillez lire le chapitre Utilisation de DeviceLock Group Policy Manager de ce manuel.

Fast servers first (Les serveurs rapides d'abord)

DeviceLock Service peut choisir le DeviceLock Enterprise Server le plus rapide parmi ceux disponibles dans la liste de serveurs.

Lorsque ce paramètre est activé, l'ensemble des serveurs spécifiés dans le paramètre **DeviceLock Enterprise Server(s)** est réparti en trois groupes en fonction de leur vitesse de réseau, et la préférence est accordée au plus rapide d'entre eux. Si aucun des serveurs du groupe le plus rapide n'est disponible, DeviceLock Service essaie de sélectionner un serveur dans le groupe suivant, et ainsi de suite.

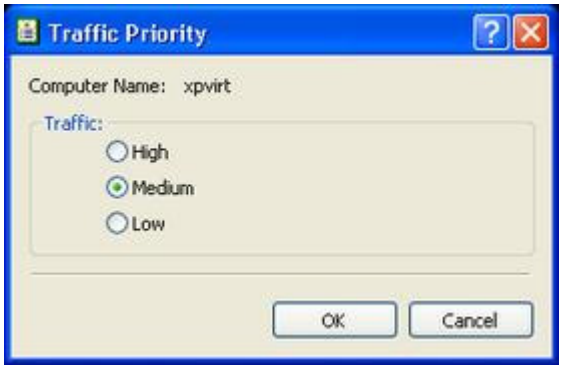
Si le paramètre **Fast servers first** est désactivé, DeviceLock Service sélectionne au hasard un serveur dans la liste.

Ce paramètre n'est efficace que si le paramètre **DeviceLock Enterprise Server(s)** comporte plus d'un serveur.

Traffic Priority (Priorité de trafic)

DeviceLock prend en charge la configuration de trafic, qui permet de définir des limites de bande passante pour l'envoi des journaux d'audit et de réplication de DeviceLock Service à DeviceLock Enterprise Server.

Vous pouvez définir trois types de priorité de trafic: Haute, moyenne et basse.



Lorsque vous sélectionnez **Haute**, vous pouvez utiliser 100 % de la bande passante. Pour réduire le trafic à 50 % de la bande passante, sélectionnez **Moyenne**. Sélectionnez **Basse** pour limiter le trafic à 10% de la bande passante.

Remarque: les priorités moyenne et basse ne fonctionnent que si le composant Quality of Service Packet Scheduler (QoS Packet Scheduler) est installé sur l'ordinateur exécutant DeviceLock Service. Sinon, le paramètre **Traffic priority** est désactivé et le trafic occupe 100 % de la bande passante. Pour plus d'informations sur la QoS, reportez-vous à l'article en ligne de Microsoft.

Always show tray icon

Utilisez cette option pour activer ou désactiver l'affichage de l'icône de DeviceLock Tray Notification Utility situé dans la zone de notification de la barre des tâches des ordinateurs client. Les utilisateurs finaux travaillant sur des ordinateurs client peuvent rafraîchir le statut de connexion (en ligne ou hors ligne) de DeviceLock Service. Pour ce faire, il leur suffit de cliquer droit sur l'icône de DeviceLock Tray Notification Utility situé dans la zone de notification de la barre des tâches, puis de cliquer sur **Refresh Current State**. Les utilisateurs finaux peuvent aussi cliquer sur l'icône de DeviceLock Tray Notification Utility pour afficher la dernière bulle de message de DeviceLock située dans la zone de notification d'un ordinateur client.

Pour activer ou désactiver l'affichage de l'icône de DeviceLock Tray Notification Utility, cliquez droit sur **Always show tray icon**, puis cliquez sur **Enable**/**Disable** ou double-cliquez sur **Always show tray icon**.

Archives content inspection on read

Cette option permet d'activer et de désactiver la vérification des fichiers contenus dans les archives lorsqu'un utilisateur essaie de lire des fichiers archivés. Pour plus d'informations, veuillez lire la description de la fonction Vérification des fichiers contenus dans les archives. Pour activer ou désactiver la vérification du contenu des fichiers archivés, faites un clic droit sur **Archives content inspection on read**, puis sur **Enable**/**Disable**, ou double-cliquez tout simplement sur **Archives content inspection on read**.

Remarque: La vérification des images incorporées dans des documents PDF, RTF et Microsoft Office ne pourra pas s'effectuer si cette option est désactivée.

Archives content inspection on write

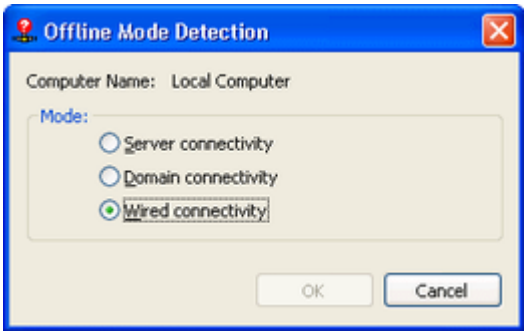
Cette option permet d'activer et de désactiver la vérification des fichiers contenus dans les archives lorsqu'un utilisateur essaie d'écrire des fichiers archivés. Pour plus d'informations, veuillez lire la description de la fonction Vérification des fichiers contenus dans les archives. Pour activer ou désactiver la vérification du contenu des fichiers archivés, faites un clic droit sur **Archives content inspection on write**, puis sur **Enable**/**Disable**, ou double-cliquez tout simplement sur **Archives content inspection on write**.

Remarque: La vérification des images incorporées dans des documents PDF, RTF et Microsoft Office ne pourra pas s'effectuer si cette option est désactivée.

Offline mode detection

Utilisez cette option pour configurer les paramètres de détection de mode hors ligne. Vous pouvez définir les caractéristiques du réseau que DeviceLock utilise pour détecter le statut de connexion (en ou hors ligne). Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client.

Pour configurer les paramètres de détection de mode hors ligne, cliquez droit sur **Offline mode detection**, puis cliquez sur **Properties** ou double-cliquez sur **Offline mode detection**.



Vous pouvez choisir l'une ou l'autre des options suivantes:

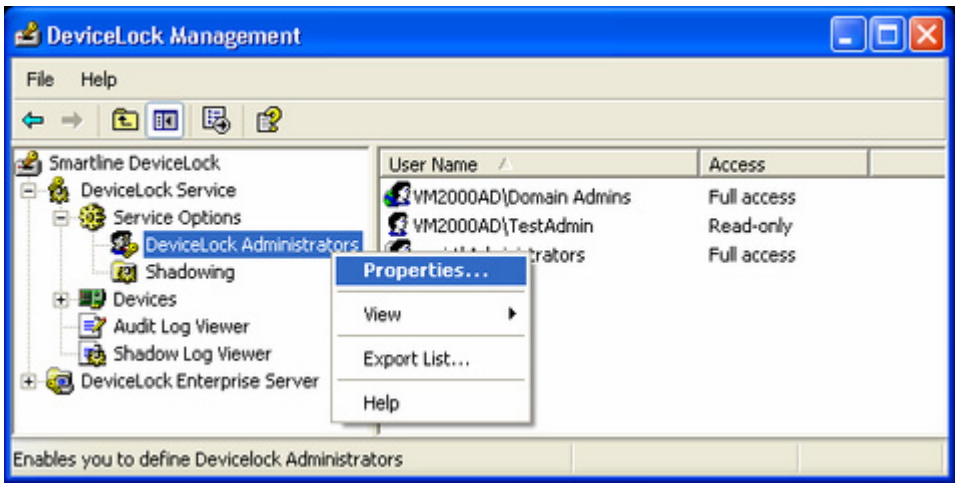
OPTION	DESCRIPTION
Server connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de sa capacité (ou non) à se connecter au DeviceLock Enterprise Server indiqué. Autrement dit, un ordinateur client fonctionne en mode en ligne s'il peut se connecter à l'un ou l'autre des DeviceLock Enterprise Server indiqués et leur envoyer des journaux d'audit et de réplication. Un ordinateur client fonctionne en mode hors ligne s'il ne peut s'identifier auprès des DeviceLock Enterprise Server indiqués ou si tous les DeviceLock Enterprise Server indiqués sont

OPTION	DESCRIPTION
	indisponibles en même temps. **Pratiques éprouvées:** La meilleure façon pour fiabiliser la communication client/serveur est d'utiliser l'authentification par DeviceLock Certificate. Pour l'authentification des certificats client/serveur, la clé publique doit être installée sur les ordinateurs client, alors que la clé privée doit être installée sur les DeviceLock Enterprise Server. Si le certificat (la clé privée) n'est installé que sur le DeviceLock Enterprise Server, le serveur refusera les connexions et les ordinateurs client fonctionneront en mode hors ligne. Si le certificat (la clé publique) n'est installé que sur les ordinateurs client, le serveur et le client s'identifieront l'un l'autre une fois la connexion établie, même si ce type d'authentification est moins sûr que l'authentification à base de certificats. Pour en savoir plus sur les DeviceLock Certificates, consultez le chapitre «Certificats DeviceLock.»
Domain connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de sa capacité (ou non) à se connecter au contrôleur de domaine Active Directory approprié (à un contrôleur de domaine du domaine auquel l'ordinateur client appartient). Dans ce cas de figure, un ordinateur client fonctionne en mode en ligne s'il peut se connecter au contrôleur de domaine approprié. Un ordinateur client fonctionne en mode hors ligne dès lors que le contrôleur de domaine approprié n'est plus disponible. *Un ordinateur client non relié à un domaine (un groupe de travail ou un ordinateur autonome) fonctionne toujours en mode hors ligne.*
Wired connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de la connexion (ou non) du câble de réseau au NIC (pour Network Interface Card, ou carte d'interface réseau). Il s'agit de la méthode la plus simple et la moins sure pour détecter le statut de connexion. Dans ce cas de figure, un ordinateur client fonctionne en mode en ligne si le câble de réseau est connecté au NIC. Un ordinateur client fonctionne en mode hors ligne si le câble de réseau est déconnecté du NIC. Remarque: les connexions à des réseaux sans fils (Wi-Fi, etc.) et les connexions modem sont ignorées. Cette option est sélectionnée par défaut.

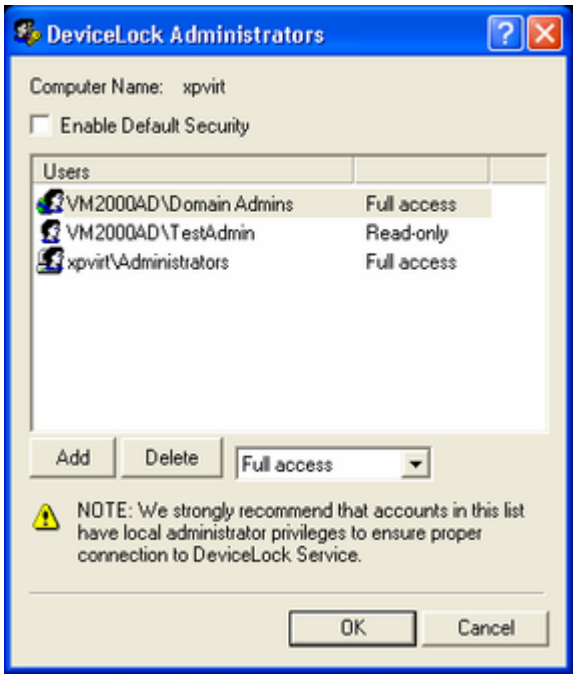
Pour en savoir plus sur les politiques hors ligne de DeviceLock, consultez le chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).»

DeviceLock Administrators

Ce paramètre permet de définir la liste des comptes dotés de droits d'accès d'administrateur à DeviceLock Service.



Utilisez le menu contextuel disponible en cliquant droit sur l'élément **DeviceLock Administrators** pour ouvrir la boîte de dialogue de configuration.



Par défaut, la configuration de sécurité de DeviceLock s'appuie sur les ACL (Access Control Lists, ou listes de contrôle d'accès) de Windows. Un utilisateur sans privilèges d'administration ne peut pas se connecter à DeviceLock Service, modifier ses paramètres ou le supprimer. Tout est contrôlé par le sous-système de sécurité de Windows.

Pour activer la sécurité par défaut liée aux ACL de Windows, cochez la case **Enable Default Security**.

Remarque: Comme indiqué dans la section Mesures de sécurité de base recommandées de ce manuel, il est fortement déconseillé d'accorder des privilèges d'administration des machines aux utilisateurs habituels.

Les utilisateurs dotés de privilèges d'administrateur local (p.ex. les membres du groupe Administrators local) peuvent se connecter à DeviceLock Service à l'aide d'une console de gestion et changer les paramètres d'autorisation, d'audit et autres. Qui plus est, ces utilisateurs peuvent désinstaller DeviceLock de leurs ordinateurs, désactiver ou supprimer DeviceLock Service, modifier les clés de registre d'un service, en supprimer le fichier exécutable, etc. En d'autres termes, les utilisateurs disposant de privilèges d'administrateur local peuvent déjouer la sécurité par défaut liée aux ACL de Windows.

Cependant, si pour une raison ou pour une autre, des utilisateurs de votre réseau possèdent ces privilèges sur leurs ordinateurs locaux, DeviceLock fournit cette fois un autre niveau de protection, dénommé DeviceLock Security. Lorsque DeviceLock Security est activé, personne hormis les utilisateurs autorisés ne peut se connecter à DeviceLock Service, l'interrompre ou le désinstaller. Même les membres du groupe Administrators local (s'ils ne figurent pas dans la liste des administrateurs DeviceLock autorisés) sont incapables de déjouer DeviceLock Security.

Pour activer DeviceLock Security, décochez la case **Enable Default Security**.

Vous devez alors préciser les comptes autorisés (les utilisateurs et/ou les groupes) qui peuvent administrer DeviceLock Service. Pour ajouter un nouvel utilisateur ou un nouveau groupe à la liste de comptes, cliquez sur le bouton **Add**. Vous pouvez ajouter plusieurs comptes en même temps.

Pour supprimer une entrée de la liste des comptes, utilisez le bouton **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Pour définir les actions d'administration de DeviceLock qu'un utilisateur ou un groupe d'utilisateurs est en droit d'effectuer, définissez les droits correspondants:

- **Full access**: permet l'accès libre à DeviceLock Service. Les utilisateurs peuvent modifier les paramètres d'autorisation, d'audit et autres, ainsi que supprimer et mettre à jour DeviceLock Service.
- **Change**: permet de modifier l'accès à DeviceLock Service. Les utilsateurs peuvent changer les paramètres, ainsi qu'installer et désinstaller DeviceLock Service, mais ils ne peuvent pas ajouter de nouveaux utilisateurs à la liste des comptes autorisés susceptibles d'administrer DeviceLock Service ou changer les droits d'accès pour les utilisateurs existants dans cette liste.
- **Read-only**: permet de n'activer les paramètres d'autorisation, d'audit et autres qu'en lecture seule. Les utilisateurs peuvent lancer des rapports et afficher les paramètres définis, mais ils ne peuvent rien modifier, ni supprimer/mettre à jour DeviceLock Service.

Remarque: Nous conseillons fortement d'accorder des privilèges d'administrateur local aux comptes figurant dans cette liste car, dans certains cas, il peut s'avérer nécessaire de disposer de droits d'accès au Windows Service Control Manager (SCM) et aux ressources de réseau partagées pour installer, mettre à jour et désinstaller DeviceLock Service.

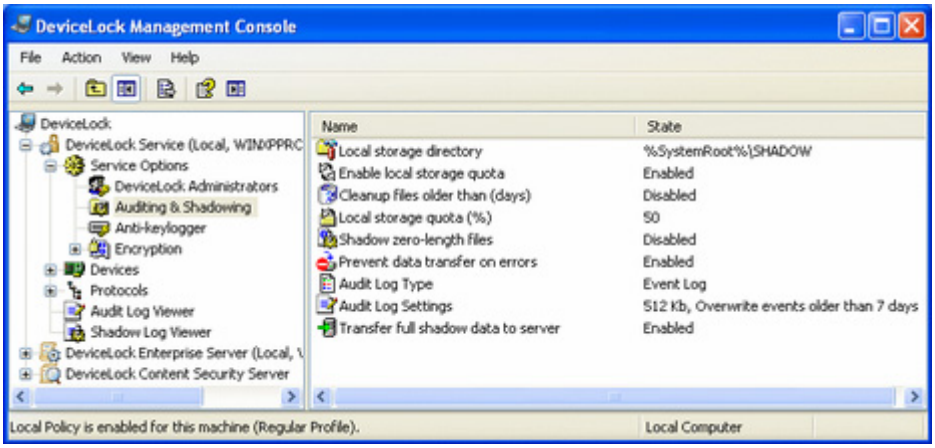
Voici juste un exemple correct de définition de liste d'administrateurs de DeviceLock : ajouter un groupe Domain Admins doté de tous les droits d'accès. Etant donné que Domain Admins est membre du groupe local Administrators sur chacun des ordinateurs du domaine, tous les membres de Domain Admins bénéficieront d'un accès libre à DeviceLock Service sur chacun des ordinateurs. Cependant, les autres membres du groupe local Administrators ne seront pas en mesure d'administrer DeviceLock Service ou de le désactiver.

De même, le fait de cocher la case **Enable Unhook Protection** (activer protection anti-hameçonnage) permet d'activer une protection optionnelle contre les techniques anti-rootkit susceptibles d'être utilisées pour désactiver volontairement DeviceLock Service. Lorsque cette protection est activée, le DeviceLock Driver contrôle l'intégrité de son code. En cas de violation, DeviceLock oblige Windows à fermer pour erreur irrécupérable (BSOD).

Remarque: Certains antivirus, pare-feux et autres logiciels tiers peu évolués risquent d'entrer en conflit avec la protection anti-hameçonnage et d'entraîner des erreurs irrécupérables (BSOD). Nous recommandons d'activer cette protection uniquement pour les systèmes ayant déjà fait l'objet de tests en la matière.

Auditing & Shadowing (Audit et réplication)

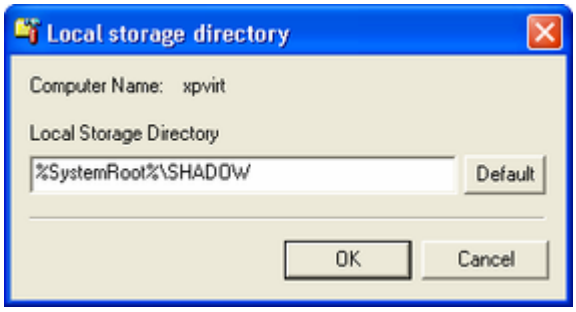
Ces paramètres permettent de peaufiner l'audit et la réplication dans DeviceLock Service.



Utilisez le menu contextuel accessible par simple clic droit de votre souris sur chaque paramètre.

Local storage directory (Répertoire de stockage local)

Utilisez ce paramètre pour définir le répertoire de stockage des données de cache (pour réplication et analyse de contenu) sur le disque local.



Par défaut, DeviceLock Service stocke les données de cache (pour réplication et analyse de contenu) dans le répertoire ***%SystemRoot%\SHADOW*** de l'ordinateur local. %SystemRoot% est une variable d'environnement standard signifiant le chemin d'accès vers le répertoire racine de Windows (C:\Windows, par exemple). Vous pouvez spécifier n'importe quel répertoire sur un disque dur localement accessible.

Ce répertoire est protégé par DeviceLock Service pour en interdire l'accès aux utilisateurs communs.

Vérifiez qu'il y a assez d'espace disque pour stocker les données (si l'utilisateur transfère 1Go vers une clé USB, il vous faudra environ 2Go d'espace disque local disponible).

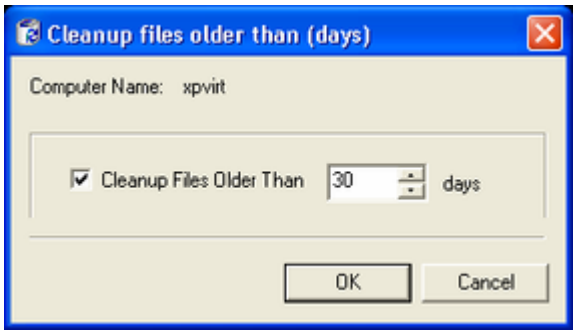
Enable local storage quota (Activer les quotas de stockage local)

Activez ce paramètre pour autoriser le nettoyage automatique des données de cache (pour réplication et analyse de contenu) stockées localement.

Lorsque ce paramètre est activé, vous pouvez aussi configurer les paramètres **Cleanup files older than (days)** et **Local storage quota (%)** (voir ci-dessous).

Cleanup files older than (days) (Supprimer les fichiers de plus de (jours))

Vous pouvez définir le nombre de jours devant s'écouler avant toute suppression automatique des données de cache (pour réplication et analyse de contenu) du stockage local.



Cochez **Cleanup Files Older Than** et spécifiez le nombre de jours devant s'écouler avant tout nettoyage automatique.

Local storage quota (%) (Quota de stockage local (%))

Vous pouvez définir un quota de disque pour les données de cache (pour réplication et analyse de contenu).

Précisez le pourcentage maximal (de 5 à 100) d'espace disque disponible utilisable pour les données de cache dans le paramètre **Local Storage Quota**.

Si la fonction quota n'est pas utilisée (le paramètre **Enable local storage quota** est désactivé), DeviceLock Service utilise toute l'espace disponible sur le disque qui contient le répertoire spécifié dans le paramètre **Local storage directory**.

Lorsque la taille totale du répertoire spécifié dans le paramètre **Local storage directory** atteint le quota, DeviceLock Service commence à supprimer les données anciennes (si le paramètre **Cleanup files older than (days)** est activé) ou interrompt la réplication des données (si le paramètre **Cleanup files older than (days)** est désactivé ou s'il n'y a rien à supprimer).

Shadow zero-length files (Réplication des fichiers de taille nulle)

Activez ce paramètre pour permettre la réplication de fichiers de taille nulle.

Même si le fichier ne contient aucune donnée, il reste possible de transférer des informations dans le nom et le chemin d'accès (jusqu'à plusieurs kilo-octets), d'où l'utilité d'activer la réplication pour les fichiers de taille nulle.

Prevent data transfer on errors

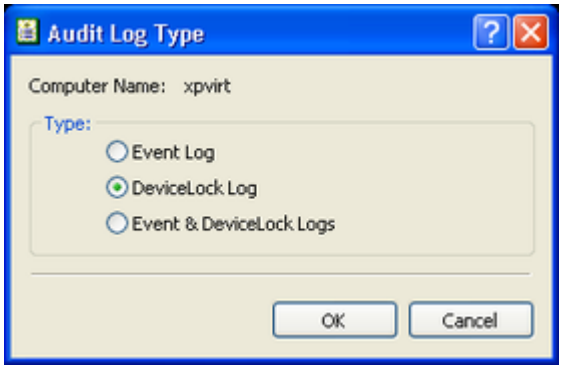
L'activation de ce paramètre permet d'empêcher les utilisateurs d'inscrire des données si la réplication ou l'analyse de contenu est impossible.

D'où la certitude que les utilisateurs ne peuvent transférer des données que si la réplication et les règles fonctionnelles fonctionnent correctement (il y a assez d'espace disque local pour stocker les données du cache, par exemple).

Lorsque le paramètre **Prevent data transfer on errors** est activé, la taille totale du répertoire spécifié dans le paramètre **Local storage directory** atteint le quota fixé dans **Local storage quota (%)** et aucune donnée ne peut plus être supprimée, DeviceLock Service arrête alors la réplication et l'analyse de contenu, et bloque toute tentative de copie des données.

Audit Log Type (Type de journal d'audit)

Grâce à ce paramètre, vous pouvez définir le journal à utiliser pour stocker les données d'audit.

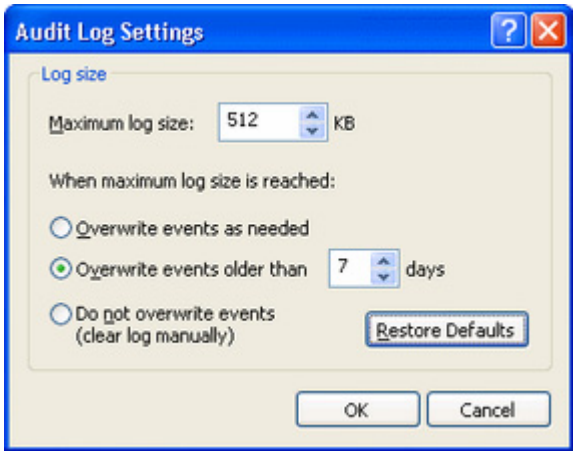


Les trois options envisageables sont les suivantes:

- **Event Log**: seul le journal des événements de Windows local standard est utilisé pour stocker les données d'audit.
- **DeviceLock Log**: seul le journal propriétaire protégé est utilisé pour stocker les données d'audit. Les données de ce journal sont envoyées à DeviceLock Enterprise Server et stockées de façon centralisée dans la base de données.
- **Event & DeviceLock Logs**: les deux journaux sont utilisés pour stocker les données d'audit.

Audit Log Settings

Utilisez **Audit Log Settings** pour indiquer la taille maximum du journal d'audit et écraser les options.



Pour obtenir une description détaillée des paramètres de journal d'audit, reportez-vous au chapitre intitulé «Audit Log Settings (Service).»

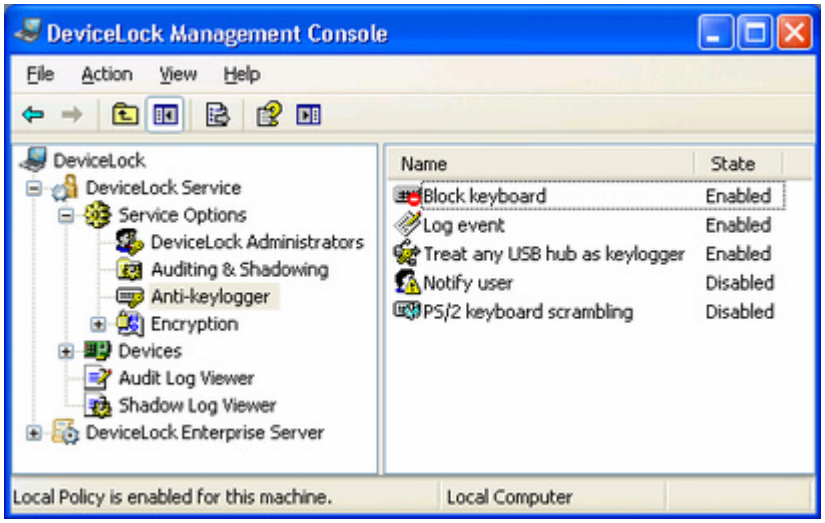
Transfer shadow data to server

Ce paramètre permet d'activer ou de désactiver le déplacement de toutes les données de réplication vers DeviceLock Enterprise Server. Si la fonction **Transfer shadow data to server** est désactivée, seules les données d'audit du journal propriétaire (si ce journal est utilisé) seront envoyées à DeviceLock Enterprise Server, la totalité des données de réplication restant stockées au niveau local sans être transférées au serveur.

Anti-keylogger

Ces paramètres permettent d'affiner la capacité qu'a DeviceLock de détecter les keyloggers matériels et de définir ce que DeviceLock Service doit faire lorsqu'il en détecte un.

Les keyloggers matériels sont des périphériques qui enregistrent les pressions de touches. DeviceLock Service peut détecter les keyloggers USB et bloquer les claviers qui leurs sont connectés. DeviceLock Service peut également bloquer les keyloggers PS/2.



Ouvrez le menu contextuel accessible par simple clic droit de votre souris sur n'importe quel paramètre.

Block keyboard (Blocage du clavier)

Activez ce paramètre pour bloquer le clavier connecté au keylogger USB matériel en cas de détection d'un keylogger.

Etant donné que DeviceLock Service démarre avant que l'utilisateur ne se connecte à Windows, il peut bloquer le clavier et empêcher l'utilisateur de saisir le mot de passe.

Remarque: Certains keyloggers matériels continuent à enregistrer les pressions de touches même si le clavier est bloqué et ne fonctionne pas sous Windows. Ceci parce que de tels keyloggers constituent des dispositifs autonomes et ne nécessitent pas de SE ou de lecteurs particuliers.

Log event (Evénement de journal)

Vous pouvez demander à DeviceLock Service d'inscrire un événement dans le journal d'audit lorsque le keylogger USB matériel est détecté.

Treat any USB hub as keylogger (Traiter n'importe quel hub USB en tant que keylogger)

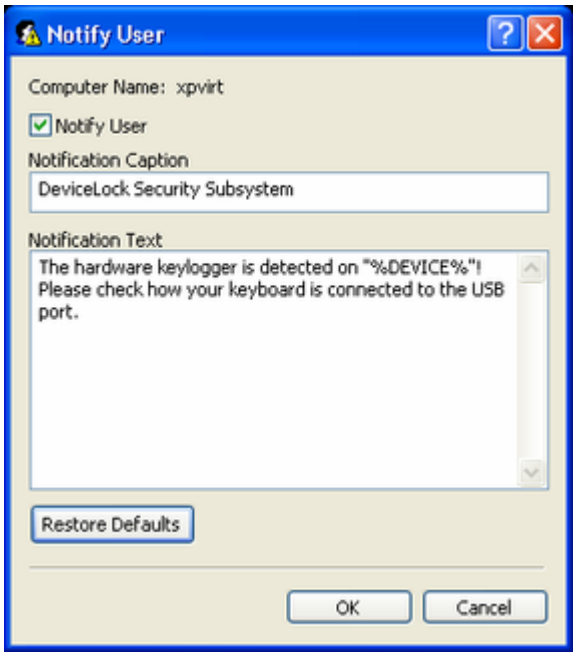
Une fois ce paramètre activé, vous pouvez commander à DeviceLock Service de traiter tous les hubs USB externes auxquels le clavier est connecté comme des keyloggers matériels.

Sinon, DeviceLock Service détecte uniquement les keyloggers des hubs qui existent dans sa base de données interne.

Notify user (Avertir l'utilisateur)

Vous pouvez définir un message personnalisé à l'intention des utilisateurs lorsque DeviceLock Service détecte des keyloggers USB matériels.

Etant donné que DeviceLock Service démarre avant que l'utilisateur ne se connecte à Windows, ce message peut avertir l'utilisateur et l'empêcher de saisir le mot de passe sur le clavier connecté au keylogger USB.



Pour permettre l'affichage du message personnalisé, cochez la case **Notify User**.

Vous pouvez aussi définir d'autres paramètres, notamment:

- **Notification Caption**: le texte sera affiché sous forme de titre. Vous pouvez utiliser les macros prédéfinies au sein du texte **%DEVICE%** afin d'insèrer le nom du clavier (p.ex. Clavier USB) reçu du système.
- **Notificaiton Text**: le texte principal du message. Vous pouvez utiliser les macros prédéfinies décrites ci-dessus au sein du texte.

PS/2 keyboard scrambling (Brouillage des claviers PS/2)

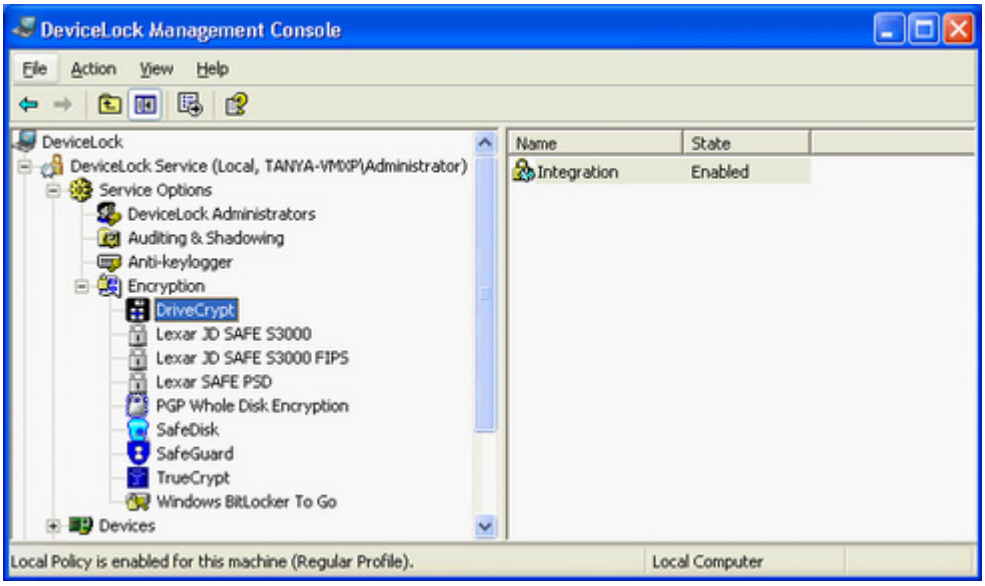
Une fois ce paramètre activé, vous pouvez empêcher les keyloggers PS/2 d'enregistrer les pressions de touches. DeviceLock Service est incapable de détecter les keyloggers PS/2 et d'avertir les utilisateurs de leur présence mais il brouille les entrées des claviers PS/2 et force les keyloggers PS/2 (le cas échéant) à enregistrer des informations parasites au lieu des pressions de touches réelles.

Remarque: Si le brouillage de clavier PS/2 est activé lors d'un travail avec le commutateur PS/2 KVM, le basculement entre les ordinateurs ne peut pas s'effectuer à partir du clavier.

Encryption (Cryptage)

DeviceLock Service peut détecter les disques (clé USB et autres périphériques à media amovibles) cryptés par des produits tiers et leur appliquer des autorisations «cryptées» spéciales.

Cette fonction permet de définir des politiques de contrôle d'accès plus souples et d'empêcher l'écriture de données sensibles sur un média non crypté.



En matière de cryptage de données sur des dispositifs de stockage amovibles, DeviceLock est actuellement compatible avec les produits tiers suivants:

- **DriveCrypt**: DeviceLockService peut détecter les dispositifs de stockage amovibles cryptés avec DriveCrypt et leur appliquer des autorisations de «cryptage» spéciales lorsque le produit DriveCrypt est installé sur l'ordinateur où s'exécute DeviceLock Service et à condition que la case **Integration** soit cochée. Pour plus d'informations sur DriveCrypt, veuillez consulter: http://www.securstar.com.
- **Lexar JD SAFE S3000** et **Lexar JD SAFE S3000 FIPS**: DeviceLock Service peut détecter les clés USB Lexar™ JumpDrive SAFE S3000 (homologuées FIPS et/ou normales) et leur appliquer des autorisations «cryptées» spéciales lorsqu'un utilisateur branche ce type de périphérique sur un ordinateur exécutant DeviceLock Service et à condition que la case **Integration** soit cochée. Pour plus d'informations sur Lexar™ JumpDrive SAFE S3000, veuillez consulter le site web de Lexar: http://www.lexar.com/products/enterprise-usb-solutions.
- **Lexar SAFE PSD**: DeviceLock Service peut détecter les lecteurs flash Lexar™ SAFE PSD S1100 USB et leur appliquer des autorisations de «cryptage» spéciales lorsqu'un

utilisateur branche un périphérique sur un ordinateur où s'exécute DeviceLock Service et à condition que la case **Integration** soit cochée. Pour plus d'informations sur Lexar SAFE PSD S1100, veuillez consulter le site Web de Lexar: http://www.lexar.com/about/newsroom/press-releases/lexar-begins-shipping-its-award-winning-safe-psd-s1100-secure-enterpri.

- **PGP Whole Disk Encryption**: DeviceLockService peut détecter les dispositifs de stockage amovibles cryptés avec PGP et leur appliquer des autorisations de «cryptage» spéciales lorsque le produit PGP® Whole Disk Encryption est installé sur l'ordinateur où s'exécute DeviceLock Service et à condition que la case **Integration** soit cochée. Pour obtenir des instructions détaillées sur le mode d'installation et d'utilisation de PGP® Whole Disk Encryption avec DeviceLock, veuillez consulter le Guide d'intégration de PGP/DeviceLock créé par PGP. Pour plus d'informations sur PGP® Whole Disk Encryption, veuillez consulter le site Web de PGP: http://www.pgp.com/products/wholediskencryption/index.html.
- **SafeDisk**: DeviceLock Service peut détecter les conteneurs SafeDisk cryptés (stockés sur des clés USB et d'autres supports amovibles) et appliquer des autorisations «cryptées» spéciales en cas d'activation de l'option **Integration**. Ces autorisations «cryptées» permettent par exemple de n'écrire que sur les périphériques amovibles cryptés et de refuser l'accès en écriture sur les supports non cryptés. Pour en savoir plus sur ViPNet Safe Disk, veuillez consulter le site Web suivant http://www.infotecs.biz/Soft/safe_disk.htm.

  Remarque: Pour accéder aux conteneurs SafeDisk et travailler avec leurs contenus, les utilisateurs doivent au moins disposer d'un accès en lecture aux périphériques amovibles non cryptés.

- **SafeGuard** :DeviceLock Service peut détecter les disques cryptés Sophos SafeGuard Easy (clés USB et autres supports amovibles) et appliquer des autorisations «cryptées» spéciales en cas d'activation de l'option **Integration**. Ces autorisations «cryptées» permettent par exemple de n'écrire que sur les périphériques amovibles cryptés et de refuser l'accès en écriture sur les supports non cryptés. Pour plus d'informations sur SafeGuard Easy, visitez le site Web Sophos.
- **TrueCrypt**: DeviceLockService peut détecter les dispositifs de stockage amovibles cryptés avec TrueCrypt et leur appliquer des autorisations de «cryptage» spéciales lorsque le produit TrueCrypt est installé sur l'ordinateur où s'exécute DeviceLock Service et à condition que la case **Integration** soit cochée. Pour en savoir plus sur TrueCrypt, consultez le site Web de TrueCrypt: http://www.truecrypt.org/.

  Remarque: Si le type de volume est «**File-hosted (container)**», l'utilisateur doit disposer au moins d'un accès en lecture seule aux dispositifs amovibles non cryptés pour avoir accès à ce volume et pouvoir travailler avec son contenu.

- **Windows BitLocker To Go**: DeviceLock Service est en mesure de détecter des lecteurs cryptés par Windows BitLocker To Go et d'y appliquer des permissions de cryptage spéciales si l'option **Integration** est activée. Pour plus d'informations sur la fonction BitLocker Drive Encryption de Windows 7, veuillez vous reporter à la section Microsoft documentation.

Remarque: Si l'intégration à Windows BitLocker To Go est activée, le paramètre **Deny write access to removable drives not protected by BitLocker** (dans **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives**) ne peut pas être activé.

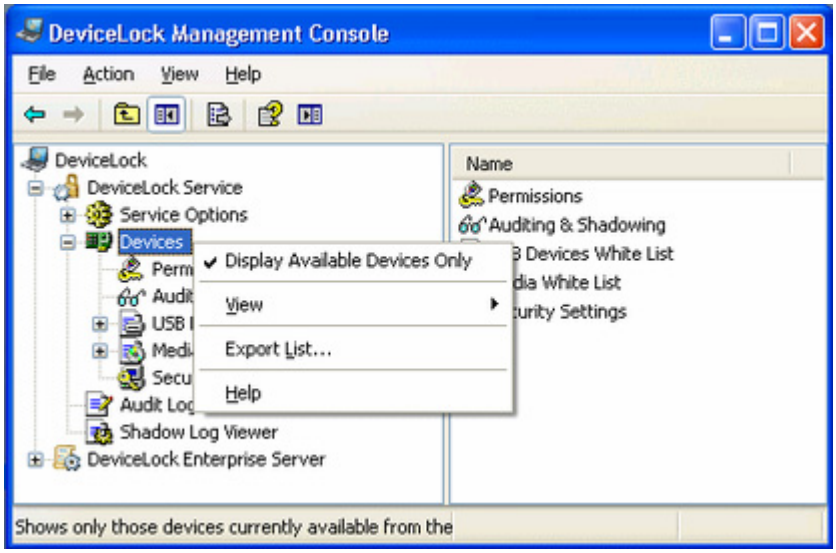
Si vous ne souhaitez pas autoriser DeviceLock Service à détecter un des produits de cryptage repertoriés ci-dessus et à appliquer des autorisations de «cryptage» spéciales pour les dispositifs de stockage cryptés avec ces produits, décochez **Integration** sous la section du produit dans la console de gestion.

Pour plus d'informations sur les autorisations de «cryptage», veuillez consulter le chapitre Autorisations de ce manuel.

Remarque: DeviceLock n'est pas fourni avec des produits de cryptage tiers et n'en nécessite pas pour fonctionner. Le fonctionnement intégré de DeviceLock et d'un produit de cryptage tiers est disponible uniquement lorsque le produit tiers a été corectement installé et configuré et qu'il est exécuteé sur le même ordinateur que DeviceLock Service.

Devices (Périphériques)

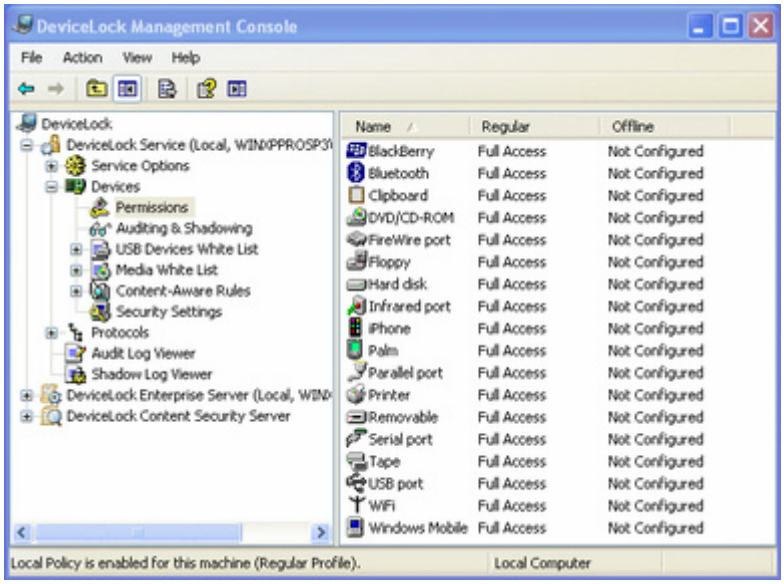
Les paramètres de configuration disponibles dans cet élément permettent l'accès aux fonctionnalités principales de DeviceLock: autorisations, audits, réplication, listes blanches et ainsi de suite.



Utilisez le menu contextuel disponible en cliquant droit sur l'élément **Devices** pour accéder à la case **Display Available Devices Only**. Si elle est cochée, DeviceLock Management Console ne montre que les types de périphériques actuellement disponibles sur l'ordinateur local. Autrement, une liste exhaustive de tous les types de périphériques que peut gérer DeviceLock apparaît dans la fenêtre. Ce listing est particulièrement utile lorsque vous voulez affecter des autorisations à des types de matériel qui ne sont pas encore installés, ou qui sont déconnectés de l'ordinateur au moment considéré.

Permissions (Autorisations) (Regular Profile)

Il existe une liste de types de matériel pour lesquels vous pouvez définir des autorisations au niveau de l'utilisateur.



Remarque: Lorsque vous configurez des autorisations pour un type de périphérique, vous les configurez pour tous les périphériques de ce type. Il est impossible de configurer des autorisations différentes pour deux matériels s'ils sont du même type (p. ex. s'il s'agit dans les deux cas d'un lecteur amovible). Pour définir des autorisations différentes pour des périphériques USB de même type, utilisez la fonctionnalité de la White List.

Le contrôle est effectué au niveau de l'interface (du port), et au niveau du type. Certains périphériques sont soumis à des vérifications aux deux niveaux, d'autres à un seul.

Pour plus d'informations sur la façon dont fonctionne le contrôle d'accès, veuillez vous reporter au chapitre Contrôle d'accès géré de ce manuel.

Les types de périphériques que DeviceLock peut gérer sont les suivants:

- **BlackBerry** (au niveau du type): inclut tous les périphériques BlackBerry, quel que soit le type d'interface de connexion (USB, Bluetooth) à l'ordinateur.
- **Bluetooth** (au niveau du type): concerne tous les périphériques Bluetooth, quel que soit le type d'interface de connexion (USB, PCMCIA, etc.) à l'ordinateur.
- **Clipboard**: y compris le presse-papiers de Windows. DeviceLock contrôle les opérations de collage des données placées dans le presse-papiers.
- **DVD/CD-ROM** (au niveau du type): concerne tous les périphériques CD/DVD (lecteurs et graveurs) internes et externes, quel que soit l'interface de connexion (IDE, SATA, USB, FireWire, PCMCIA, etc.).
- **FireWire port** (au niveau de l'interface): concerne tous les périphériques qu'on peut brancher à un port FireWire (IEEE 1394), à l'exception des hubs.

- **Floppy** (au niveau du type): concerne tous les lecteurs de disquette internes et externes, quelle que soit l'interface de connexion (IDE, USB, PCMCIA, etc.). Il peut arriver que certains lecteurs de disquette non-standard soient reconnus par Windows comme périphériques amovibles ; dans ce cas, DeviceLock les traite aussi comme des périphériques amovibles.
- **Hard disk** (au niveau du type): concerne tous les disques durs internes, quel que soit l'interface de connexion (IDE, SATA, SCSI, etc.). DeviceLock assimile tous les disques durs externes connectés par USB, FireWire ou PCMCIA à des périphériques Removable. DeviceLock assimile aussi certains disques durs internes (normalement SATA et SCSI) au type **Removable**: ceci peut se produire si la fonctionnalité de branchement à chaud est prise en charge par le disque, et si celui-ci ne contient pas ou n'exécute pas Windows.

  Remarque: Même si vous interdisez l'accès au type Disque Dur, les utilisateurs disposant de privilèges d'administrateurs locaux (l'utilisateur SYSTEM et les membres du groupe local Administrators) pourront toujours accéder à la partition où Windows est installé et s'exécute.

- **Infrared port** (au niveau de l'interface): concerne tous les périphériques susceptibles d'être connectés à l'ordinateur via le port infrarouge (IrDA).
- **iPhone** (au niveau du type): y compris tous les iPhone, iPod Touch et iPad. DeviceLock contrôle les périphériques iPhone, iPod Touch et iPad qui fonctionnent avec un PC via l'application iTunes ou ses API.
- **Palm** (au niveau du type): tous les périphériques Palm OS, quel que soit le type d'interface de connexion (USB, COM, IrDA, Bluetooth, WiFi) à l'ordinateur. DeviceLock contrôle les périphériques Palm OS qui fonctionnent avec un PC via l'application HotSync.
- **Parallel port** (au niveau de l'interface): concerne tous les périphériques susceptibles d'être connectés à l'ordinateur via un port parallèle (LPT).
- **Printer** (au niveau du type); ceci inclut toutes les imprimantes locales et réseau, quelle que soit l'interface de connexion (USB, LPT, Bluetooth, etc.) à l'ordinateur. Le cas échéant, DeviceLock peut aussi contrôler des imprimantes virtuelles qui n'envoient pas les documents à des périphériques réels, mais les impriment dans des fichiers (p.ex. des convertisseurs PDF).
- **Removable** (au niveau du type): concerne tous les périphériques internes et externes, quelle que soit l'interface de connexion (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc.), que Windows reconnaît comme des dispositifs amovibles (par exemple, les clés USB, les lecteurs ZIP, les lecteurs de carte, les lecteurs optomagnétiques, etc.). DeviceLock assimile tous les disques durs externes connectés par USB, FireWire ou PCMCIA à des périphériques **Removable**. DeviceLock assimile aussi certains disques durs internes (normalement SATA et SCSI) au type **Removable**: ceci peut se produire si la fonctionnalité de branchement à chaud est prise en charge par le disque, et si celui-ci ne contient pas ou n'exécute pas Windows.
- **Serial port** (au niveau de l'interface): concerne tous les périphériques susceptibles d'être connectés à l'ordinateur via un port série (COM), y compris les modems internes.

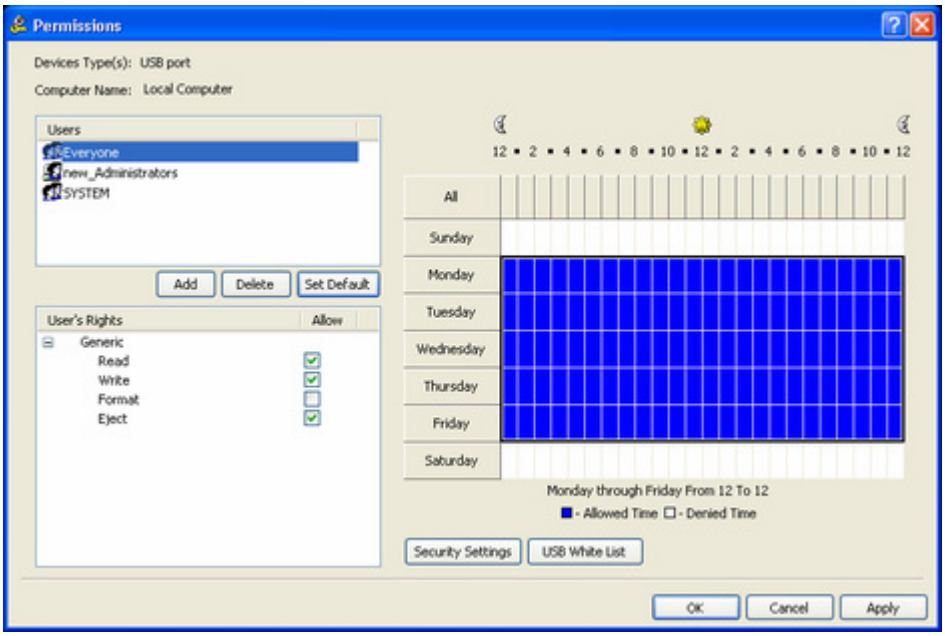
- **Tape** (au niveau du type): concerne tous les lecteurs de bande internes et externes, quelle que soit l'interface de connexion (IDE, USB, SCSI, etc.).
- **USB port** (au niveau de l'interface): concerne tous les périphériques qu'on peut brancher à un port USB, à l'exception des hubs.
- **WiFi** (au niveau du type): concerne tous les périphériques WiFi internes ou externes, quelle que soit l'interface de connexion (USB, PCMCIA, etc.) à l'ordinateur.

  Remarque: Le type WiFi permet de contrôler l'accès des utilisateurs au périphérique matériel mais pas au réseau.

- **Windows Mobile** (au niveau du type): tous les périphériques mobiles Windows, quel que soit le type d'interface de connexion (USB, COM, IrDA, Bluetooth, WiFi) à l'ordinateur. DeviceLock contrôle les périphériques mobiles Windows fonctionnant avec un PC via l'application Windows Mobile Device Center (WMDC) ou Microsoft ActiveSync ou son API.

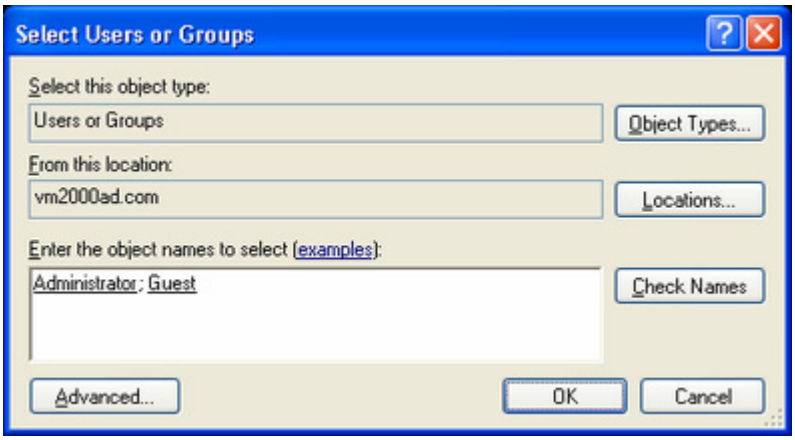
Remarque: Vous pouvez définir des autorisations différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les autorisations en ligne (Regular Profile) s'appliquent aux ordinateurs client qui fonctionnent en ligne. Les autorisations hors ligne (Offline Profile) s'appliquent aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des autorisations hors ligne, reportez-vous au chapitre intitulé «Gestion des autorisations hors ligne.»

Pour configurer des autorisations d'accès pour un type de périphérique, soulignez-le (utilisez Ctrl et/ou Maj pour sélectionner plusieurs types simultanément) puis sélectionnez **Set Permissions** à l'aide du menu contextuel disponible en cliquant droit. Vous pouvez aussi utiliser le bouton approprié sur la barre d'outils.



Les noms des utilisateurs et des groupes d'utilisateurs assignés au type de périphériques sont affiché dans la liste des comptes situé du côté gauche en haut de la boîte de dialogue **Permissions**.

Pour ajouter un nouvel utilisateur ou un nouveau groupe à la liste de comptes, cliquez sur le bouton **Add**. Vous pouvez ajouter plusieurs comptes en même temps.



Pour supprimer une entrée de la liste des comptes, utilisez le bouton **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Utilisez **Set Default** pour configurer des autorisations par défaut. Les autorisations par défaut sont activées en utilisant l'une des sélections d'accès suivantes:

COMPTE/ TYPE DE PERIPHERIQUE	TOUS	ADMINISTRATEURS	SYSTÈME
BlackBerry	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Bluetooth	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Clipboard	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content
DVD/CD-ROM	Generic: Read, Write, Eject	Generic: Read, Write, Eject	Generic: Read, Write, Eject
FireWire port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Floppy	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject

COMPTE/ TYPE DE PERIPHERIQUE	TOUS	ADMINISTRATEURS	SYSTÈME
Hard disk	Generic: Read, Write	Generic: Read, Write, Format	Generic: Read, Write, Format
Infrared port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
iPhone	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Palm	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Parallel port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Printer	Generic: Print	Generic: Print	Generic: Print
Removable	Generic: Read, Write, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format
Serial port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Tape	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
USB port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
WiFi	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Windows Mobile	Generic: Read, Write, Execute	Generic: Read, Write, Execute	Generic: Read, Write, Execute

La fonctionnalité «Contrôle temps» permet de définir les périodes pendant lesquelles un utilisateur ou un groupe d'utilisateurs choisis auront ou n'auront pas accès aux périphériques. La fenêtre «Contrôle temps» s'affiche en haut à droite de la boîte de dialogue d'autorisations. Utilisez le bouton gauche de la souris et sélectionnez la période d'autorisation. Pour sélectionner les périodes où l'accès est refusé, utilisez le clic droit de votre souris. Le cas échéant, vous pouvez également utiliser des commandes clavier – les flèches vous serviront alors à naviguer dans le tableau et la barre d'espace à basculer entre périodes autorisées/refusées.

Pour définir les actions autorisées par un utilisateur ou un groupe d'utilisateurs sur des périphériques donnés, configurez les droits et privilèges appropriés. Les droits sont répartis en trois groupes: **Generic**, **Encrypted** et **Special Permissions**. Chaque groupe dispose de son propre ensemble de droits:

- **Generic** – Les droits génériques ne s'appliquent pas aux périphériques que DeviceLock reconnaît comme des périphériques cryptés. Pour plus d'informations sur l'intégration du cryptage, veuillez consulter le chapitre Cryptage de ce manuel.

- **Read** – permet de lire les données contenues dans le périphérique. S'applique à tous les types de périphériques, à l'exception des périphériques de type Clipboard et Printer.
- **Write** – permet l'écriture de données sur le périphérique. Ce droit peut être activé pour tous les dispositifs (sauf Windows Mobile) seulement si **Read** est sélectionné dans le groupe **Generic**. Il est impossible de le désactiver pour les périphériques BlackBerry, Bluetooth, Infrared port, Parallel port, Serial port et WiFi. Lorsque **Write** est désactivé pour les ports USB et FireWire, il est possible de lire les périphériques de stockage, notamment les lecteurs flash, les disquettes, les disques durs, les DVD et CD-ROM, etc., mais pas d'y écrire. Il est également impossible d'accéder aux périphériques non destinés au stockage (imprimantes, scanners, etc.).
- **Format** – permet d'activer le formatage, la vérification et tout autre accès direct aux lecteurs cryptés. Vous ne pouvez activer ce droit que si **Read** est sélectionné dans le groupe **Generic**. Ne s'applique qu'aux types de périphériques suivants: FireWire port, Floppy, Hard disk, Removable et USB port. L'activation de ce droit pour les ports USB et FireWire affecte uniquement les dispositifs de stockage branchés sur ces ports.
- **Eject** – permet d'activer l'éjection des média. Vous ne pouvez activer ce droit que si **Read** est sélectionné dans le groupe **Generic**. Ce privilège contrôle seulement l'éjection logicielle. L'éjection manuelle par voie matérielle (c'est à dire en appuyant sur le bouton Ejecter d'un appareil) ne peut pas être empêchée. Il s'applique seulement aux types de périphériques suivants: DVD/CD-ROM, FireWire port, Floppy, Removable et USB port. L'activation de ce droit pour les ports USB et FireWire affecte uniquement les dispositifs de stockage branchés sur ces ports.
- **Execute** – permet d'activer l'exécution à distance du code du dispositif. Ne s'applique qu'aux périphériques de type Windows Mobile.
- **Print** – permet l'impression des documents. Ne s'applique qu'aux périphériques de type Printer.
- **Copy to clipboard** – permet d'activer le collage des données à partir du presse-papiers. Ne s'applique qu'aux périphériques de type Clipboard. Cette autorisation fournit automatiquement un accès total au presse-papiers.

- **Encrypted** – Les droits cryptés s'appliquent exclusivement aux périphériques que DeviceLock reconnaît comme des périphériques cryptés. Pour plus d'informations sur l'intégration du cryptage, veuillez consulter le chapitre Cryptage de ce manuel.

  - **Read** – permet la lecture de données à partir d'un dispositif crypté. Ne s'applique qu'aux dispositifs de type Removable.
  - **Write** – permet l'écriture de données sur un dispositif crypté. Vous ne pouvez activer ce droit que si **Read** est sélectionné dans le groupe **Encrypted**. Ne s'applique qu'aux dispositifs de type Removable.
  - **Format** – permet d'activer le formatage, la vérification et tout autre accès direct aux lecteurs cryptés. Vous ne pouvez activer ce droit que si **Read** est sélectionné dans le groupe **Encrypted**. Ne s'applique qu'aux dispositifs de type Removable.

- **Special Permissions** – ces droits s'appliquent uniquement aux périphériques de type iPhone, Windows Mobile, Palm et Clipboard. Les types de contenus (Calendrier, Contacts, Tâches, etc.) contrôlés avec ces droits pour les périphériques iPhone,

Windows Mobile et Palm correspondent aux mêmes types de contenus que ceux présents dans les applications HotSync, Microsoft ActiveSync et WMDC. Pour les périphériques Palm, vous pouvez activer n'importe quel droit **Write** mais à condition que le droit **Read** correspondant soit aussi activé.

- **Read Calendar** – permet de lire le calendrier sur un périphérique mobile à partir d'un PC.
- **Write Calendar** – permet d'écrire sur un calendrier de périphérique mobile à partir d'un PC.
- **Read Contact** – permet de lire des contacts sur un périphérique mobile à partir d'un PC.
- **Write Contact** – permet d'écrire des contacts sur un périphérique mobile à partir d'un PC.
- **Read E-mail** – permet de lire des e-mails sur un périphérique mobile à partir d'un PC. Pour l'iPhone, ce type de contenus représente des paramètres de compte de messagerie mais pas des messages, car iTunes ne permet pas la synchronisation des messages.
- **Write E-mail** – permet d'écrire des e-mails sur un périphérique mobile à partir d'un PC. Pour l'iPhone, ce type de contenus représente des paramètres de compte de messagerie mais pas des messages, car iTunes ne permet pas la synchronisation des messages.
- **Read Attachment** – permet de lire des pièces jointes aux e-mails sur un dispositif Windows Mobile à partir d'un PC. Vous ne pouvez activer ce droit que si **Read E-mail** est sélectionné dans le groupe **Special Permissions**.
- **Write Attachment** – permet d'écrire des pièces jointes d'e-mails sur un dispositif Windows Mobile à partir d'un PC. Vous ne pouvez activer ce droit que si **Write E-mail** est sélectionné dans le groupe **Special Permissions**.
- **Read Favorite** – permet de lire des favoris sur un périphérique Windows Mobile et iPhone à partir d'un PC.
- **Write Favorite** – permet d'écrire des favoris sur un périphérique Windows Mobile et iPhone à partir d'un PC.
- **Read File** – permet de lire des fichiers sur un périphérique mobile à partir d'un PC. Pour l'iPhone, les flux de données du type *Applications* iTune sont traités en tant que fichiers.
- **Write File** – permet d'écrire des fichiers sur un périphérique mobile à partir d'un PC. Pour un périphérique Palm, ce droit permet aussi d'activer **Write Document** dans le groupe **Special Permissions**. Pour l'iPhone, les flux de données du type *Applications* iTune sont traités en tant que fichiers.
- **Read Media** – permet d'activer la lecture de contenus média avec Windows Media Player sur un périphérique Windows Mobile et la lecture de fichiers média sur un périphérique Palm et iPhone à partir d'un PC. Vous ne pouvez activer ce droit que si **Read Files** est sélectionné dans le groupe **Special Permissions**. Pour un périphérique Windows Mobile, cette option nécessite aussi de sélectionner **Execute** dans le groupe **Generic**. Pour l'iPhone, le type de contenus de média correspond aux types iTunes suivants: Sonneries, Musique, Livres audio, Photos, Podcasts (Audio & Vidéo), Films, Séries TV, Films à louer.
- **Write Media** – permet d'activer l'écriture de contenus média avec Windows Media Player sur un périphérique Windows Mobile et l'écriture de fichiers média sur un périphérique Palm et iPhone à partir d'un PC. Vous ne pouvez activer ce droit que si **Write Files** est sélectionné dans le groupe **Special**

Permissions, et pour un périphérique Windows Mobile si **Execute** est sélectionné dans le groupe **Generic**. Pour l'iPhone, le type de contenus de média correspond aux types iTunes suivants: Sonneries, Musique, Livres audio, Photos, Podcasts (Audio & Vidéo), Films, Séries TV, Films à louer.

- **Read Backup** – permet d'activer la création de la sauvegarde iPhone par lecture des données du périphérique à partir d'un PC.

Remarque: Un iPhone fait l'objet d'une sauvegarde à chaque synchronisation avec iTunes (automatiquement lors de la première synchronisation, à chaque fois que l'utilisateur le connecte à l'ordinateur). Pour permettre une synchronization parfaite, accordez l'autorisation **Read Backup** aux utilisateurs de périphériques de type **iPhone**. Sinon, si iTunes crée automatiquement une sauvegarde iPhone, la session de synchronisation sera interrompue.

Pour éviter d'interrompre le processus de synchronisation, les utilisateurs devront configurer iTunes pour qu'il ne synchronise que le contenu auquel ils ont accès.

- **Write Backup** – permet d'activer la restauration iPhone par écriture des données de sauvegarde du périphérique à partir d'un PC.
- **Read Note** – permet d'activer la lecture de notes sur un périphérique mobile à partir d'un PC. Pour un périphérique Palm, ce droit contrôle les types de contenus Memos et Note Pad.
- **Write Note** – permet d'écrire des notes sur un périphérique mobile à partir d'un PC. Pour un périphérique Palm, ce droit contrôle les types de contenus Memos et Note Pad.
- **Read Pocket Access** – permet de lire des bases de données Pocket Access sur un dispositif Windows Mobile à partir d'un PC.
- **Write Pocket Access** – permet d'écrire dans des bases de données Pocket Access sur un dispositif Windows Mobile à partir d'un PC.
- **Read Task** – permet de lire des tâches sur un périphérique mobile à partir d'un PC.
- **Write Task** – permet d'écrire des tâches sur un périphérique mobile à partir d'un PC.
- **Read Expense** – permet de lire des données d'une application Palm Expense sur un périphérique Palm à partir d'un PC.
- **Write Expense** – permet d'écrire des données d'une application Palm Expense sur un périphérique Palm à partir d'un PC.
- **Read Document** – permet de lire des documents Palm sur un périphérique Palm à partir d'un PC. Vous ne pouvez activer ce droit que si **Read Files** est sélectionné dans le groupe **Special Permissions**.
- **Write Document** – permet d'écrire des documents Palm sur un périphérique Palm à partir d'un PC. Vous ne pouvez activer ce droit que si **Write Files** est sélectionné dans le groupe **Special Permissions**.
- **Read Unidentified Content** – permet de lire n'importe quel autre type de contenu n'appartenant à aucune catégorie sur un dispositif Windows Mobile à partir d'un PC.
- **Write Unidentified Content** – permet d'écrire n'importe quel autre type de contenu n'appartenant à aucune catégorie sur un dispositif Windows Mobile à partir d'un PC.
- **Copy Text** – permet d'activer le collage des données de texte à partir du presse-papiers.
- **Copy Image** – permet d'activer le collage des données graphiques à partir du presse-papiers.

- **Copy Audio** – permet d'activer le collage des données audio à partir du presse-papiers.
- **Copy File** – permet d'activer le collage des fichiers à partir du presse-papiers.
- **Screenshot** – permet d'activer la capture de l'écran entier, de la fenêtre active ou d'une partie quelconque de l'écran vers le presse-papiers.

Remarque: Étant donné que les captures d'écran réalisées à l'aide d'outils et d'utilitaires de capture d'écran sont directement enregistrées dans des fichiers, alors que les captures d'écran par l'intermédiaire de la touche PRINT SCREEN sont d'abord copiées dans le presse-papiers avant d'être collées dans un autre programme (à l'exemple de Microsoft Word ou Paint), différents droits d'accès sont nécessaires pour les restrictions d'accès aux captures d'écran. Pour permettre aux utilisateurs de faire des captures d'écran à l'aide d'outils et d'utilitaires de capture d'écran, il suffit de leur accorder le droit Screenshot uniquement. Pour permettre aux utilisateurs de faire des captures d'écran par l'intermédiaire de la touche PRINT SCREEN, vous devez leur accorder les droits Screenshot et Copy Image.

Un utilisateur ne disposant pas du droit Screenshot ne pourra pas réaliser de captures d'écran, ni par la touche PRINT SCREEN ni avec des outils ou utilitaires de capture d'écran.

- **Copy Unidentified Content** – permet d'activer le collage de tout autre type de contenu non classifié à partir du presse-papiers.

Remarque: Les droits Copy Text, Copy Image, Copy Audio, Copy File et Copy Unidentified Content ne contrôlent pas la copie des données vers le presse-papiers. Les utilisateurs peuvent copier des données vers le presse-papiers à leur gré, indépendamment des droits d'accès dont ils disposent.

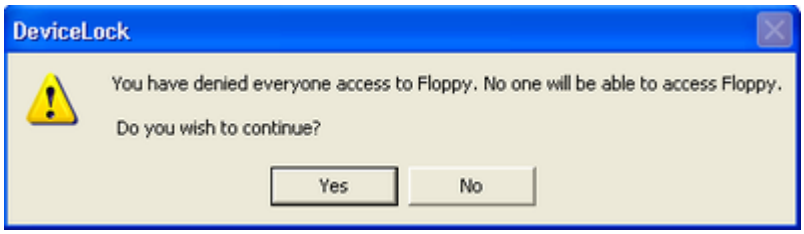
Remarque: Si l'accès (lecture et/ou écriture) à certains types de contenus est refusé lors du processus de synchronisation de l'iPhone ou du Windows Mobile, il faut rebrancher le périphérique pour pouvoir continuer à utiliser le périphérique iPhone ou Windows Mobile.

Lorsque des utilisateurs tentent de synchroniser un organisateur de poche Palm sur un réseau, et que DeviceLock refuse l'accès à certains types de contenus, la session de synchronisation est interrompue. Pour éviter une telle situation, les utilisateurs doivent configurer l'application HotSync de façon à ne synchroniser que le contenu auquel ils ont accès avant de tenter une synchronisation quelconque.

Si tous les droits sont activés pour le compte utilisateur, c'est que ce compte possède des droits de type «accès libre» à un périphérique. Si tous les droits sont désactivés pour le compte utilisateur, c'est que ce compte possède des droits de type «aucun accès» à un périphérique.

Remarque: Les droits de type «aucun accès» ont priorité sur tous les autres types de droits. Autrement dit, si le groupe auquel appartient l'utilisateur a un droit de type «aucun accès», mais que cet utilisateur a un droit de type «accès libre», l'utilisateur ne pourra pas accéder au périphérique. Si vous voulez interdire l'accès à un groupe ou à un utilisateur, il suffit de le supprimer de la liste du compte: inutile de le rajouter avec «aucun accès».

Pareillement, l'utilisateur Everyone est prioritaire sur tous les autres comptes. En d'autres termes, si Everyone a des droits de type «aucun accès», personne ne pourra accéder au périphérique.

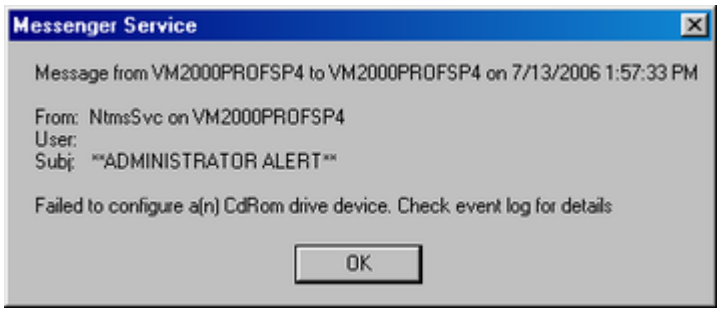


Même si vous interdisez l'accès aux disques durs, les utilisateurs disposant de privilèges d'administration locaux (l'utilisateur SYSTEM et les membres du groupe local Administrators) pourront toujours accéder à la partition où Windows est installé et s'exécute.

Il est recommandé de ne rajouter à la liste que les comptes (utilisateurs et/ou groupes) qui doivent pouvoir accéder à un périphérique. Si la liste du compte est vide (ne contient aucune donnée), personne ne pourra accéder au périphérique.

Il est aussi recommandé d'ajouter l'utilisateur SYSTEM avec droits de type «accès libre» aux disques durs et aux DVD/CD-ROM.

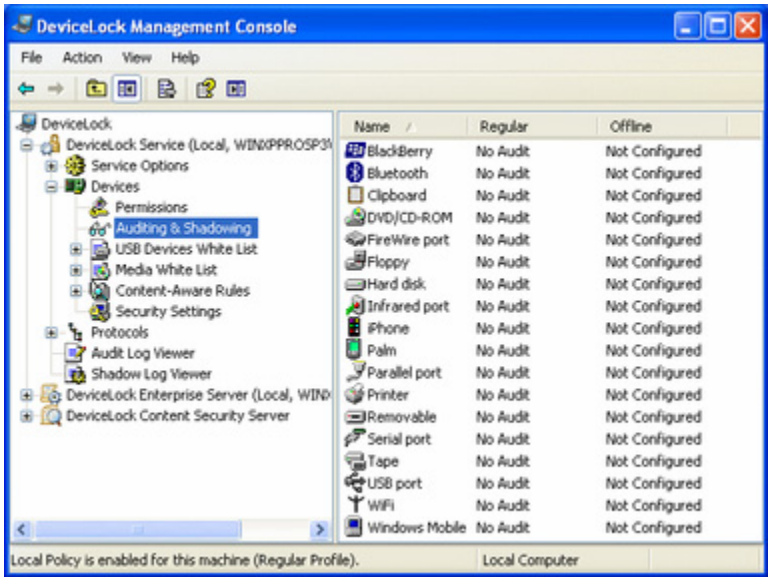
Sur certains systèmes, il est possible que les utilisateurs reçoivent le message suivant lorsqu'ils ouvrent une session.


Messenger Service
Message from VM2000PROFSP4 to VM2000PROFSP4 on 7/13/2006 1:57:33 PM
From: NtmsSvc on VM2000PROFSP4
User:
Subj: **ADMINISTRATOR ALERT**
Failed to configure a(n) CdRom drive device. Check event log for details
OK

Cela signifie que l'utilisateur SYSTEM ne peut pas accéder au DVD/CD-ROM. Pour éviter ce message, accordez des droits de type «accès libre» à l'utilisateur SYSTEM pour le DVD/CD-ROM.

Auditing & Shadowing (Audit et réplication) (Regular Profile)

Il existe une liste de types de matériels pour lesquels vous pouvez définir des règles d'audit et de réplication au niveau de l'utilisateur.



Il y a peu de différences entre la configuration des autorisations et la définition des règles d'audit et de réplication: commencez donc par lire le chapitre Permissions de ce manuel.

DeviceLock Service utilise le sous-système d'enregistrement d'événements standard de Windows pour enregistrer les informations provenant d'un périphérique. Ceci est particulièrement utile pour les administrateurs systèmes, qui peuvent ainsi utiliser tout logiciel de lecture d'enregistrement d'événements pour visualiser le journal d'événements de DeviceLock. Par exemple, vous pouvez utiliser Event Viewer standard. DeviceLock Service peut aussi utiliser son popre journal propriétaire protégé. Les données de ce journal sont envoyées à DeviceLock Enterprise Server et stockées de façon centralisée dans la base de données. Pour indiquer le journal à utiliser, définissez le paramètre **Audit log type** dans les Service Options.

DeviceLock Management Console possède également son propre visionneur d'audits intégré, qui présente les informations dans un format plus pratique. Pour plus d'informations, veuillez lire le chapitre Audit Log Viewer (Service) de ce manuel.

Pour visionner le journal de réplication stocké sur DeviceLock Enterprise Server, utilisez le Audit Log Viewer du serveur.

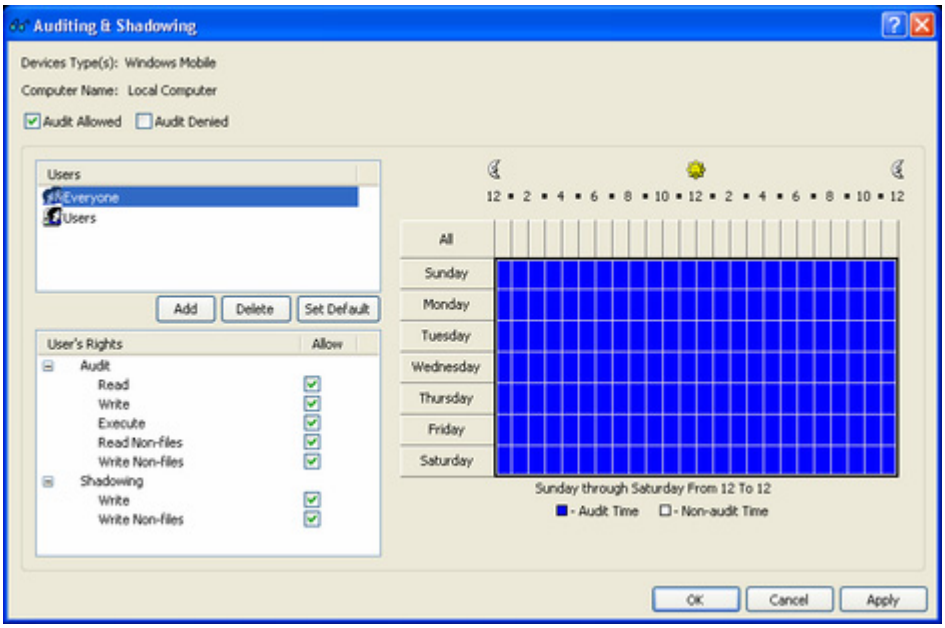
Il existe également une fonctionnalité d'audit étendue, appelée «réplication des données»: il s'agit de la capacité à restituer toute donnée copiée vers une solution de stockage externe ou transférée par un port parallèle ou série. Une copie totale des données est enregistrée. Le journal de réplication est stocké localement dans le répertoire spécial (voir Service Options) et peut être transféré vers DeviceLock Enterprise Server spécifié dans Service Options afin de le stocker dans la base de données SQL.

Pour visionner le journal de réplication stocké localement, utilisez le visionneur de journal de réplication intégré de DeviceLock Management Console. Pour plus d'informations, veuillez lire le chapitre Shadow Log Viewer (Service) de ce manuel.

Pour visionner le journal de réplication stocké sur DeviceLock Enterprise Server, utilisez le Shadow Log Viewer du serveur.

Remarque: Vous pouvez définir des règles d'audit et de réplication différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les règles d'audit et de réplication en ligne (Regular Profile) s'appliquent aux ordinateurs client qui fonctionnent en ligne. Les règles d'audit et de réplication hors ligne (Offline Profile) s'appliquent aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des règles d'audit et de réplication hors ligne, reportez-vous au chapitre intitulé «Gestion des règles d'audit et de réplication hors ligne.»

Pour définir les règles d'audit et de réplication d'un type de périphérique donné, soulignez-le (utilisez Ctrl et/ou Maj pour sélectionner plusieurs types simultanément) puis sélectionnez **Set Auditing & Shadowing** dans le menu contextuel disponible en cliquant droit. Vous pouvez aussi utiliser le bouton approprié sur la barre d'outils.



Deux types d'accès utilisateur peuvent figurer dans le journal d'audit:

- **Allowed**: toutes les tentatives d'accès qui ont été permises par DeviceLock Service: l'utilisateur a eu accès au périphérique.
- **Denied**: toutes les tentatives d'accès qui ont été bloquées par DeviceLock Service: l'utilisateur n'a pas pu accéder au périphérique.

Pour activer l'enregistrement de l'un ou l'autre de ces types d'accès, cochez **Audit Allowed** et/ou **Audit Denied**. Ces options ne sont pas liées aux utilisateurs/groupes, mais se rapportent à une classe entière de périphériques.

Les noms des utilisateurs et des groupes d'utilisateurs assignés au type de périphériques sont affichés dans la liste des comptes située en haut à gauche de la boîte de dialogue **Auditing & Shadowing**.

Pour ajouter un nouvel utilisateur ou un nouveau groupe à la liste de comptes, cliquez sur le bouton **Add**. Vous pouvez ajouter plusieurs comptes en même temps.

Pour supprimer une entrée de la liste des comptes, utilisez le bouton **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Utilisez **Set Default** pour configurer les règles d'audit et de réplication par défaut: Les membres du groupe Users et du compte Everyone disposent des droits d'audit **Read** et **Write**; ils n'ont pas accès à la réplication.

La fonctionnalité «Contrôle temps», permet de définir les périodes pendant lesquelles un utilisateur ou un groupe d'utilisateurs choisis seront ou ne seront pas soumis à la règle d'audit. La fenêtre «Contrôle temps» s'affiche en haut à droite de la boîte de dialogue **Auditing & Shadowing**. Utilisez le bouton gauche de la souris et sélectionnez la période pendant laquelle la règle est appliquée (période d'audit). Pour sélectionner une période pendant laquelle la règle n'est pas active, (période sans audit), utilisez le clic droit de votre souris. Si vous préférez, vous pouvez également utiliser des commandes clavier – les flèches vous serviront alors à naviguer dans le tableau et la barre d'espace à basculer entre périodes avec et sans audit.

Afin de définir les actions que vous souhaitez retrouver dans le journal d'audit ou le journal de réplication lors d'une connexion à un périphérique par un utilisateur ou un groupe d'utilisateurs donnés, choisissez les droits d'audit correspondants: Les droits sont répartis en deux groupes: **Audit** et **Shadowing**. Chaque groupe dispose de son propre ensemble de droits:

- **Audit** – les droits affectés à ce groupe sont responsables des actions enregistrées dans le journal de réplication.
    - **Read** – permet d'enregistrer les tentatives d'accès en lecture. Pour les périphériques de type BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port et WiFi, ce droit ne peut être activé que si **Write** est sélectionné dans le groupe **Audit**.
    - **Write** – permet d'enregistrer les tentatives d'accès en écriture. Pour les périphériques de type BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port et WiFi, ce droit ne peut être activé que si **Read** est sélectionné dans le groupe **Audit**.
    - **Print** – permet d'enregistrer les tentatives d'envois de documents aux imprimantes. Ne s'applique qu'aux périphériques de type Printer.
    - **Execute** – enregistre les tentatives d'accès pour exécuter à distance un code sur le périphérique. Ne s'applique qu'aux périphériques de type Windows Mobile.

- **Read Non-files** – permet d'enregistrer les tentatives d'accès en lecture aux objets autres que des fichiers (Calendrier, Contacts, Tâches, etc.). Ne s'applique qu'aux périphériques de types iPhone, Windows Mobile et Palm.
- **Write Non-files** – permet d'enregistrer les tentatives d'accès en écriture aux objets autres que des fichiers (Calendrier, Contacts, Tâches, etc.). Ne s'applique qu'aux périphériques de types iPhone, Windows Mobile et Palm.
- **Copy** – permet la journalisation de toutes les tentatives de collage de données à partir du presse-papiers et de capture d'écran. S'applique uniquement au presse-papiers.

- **Shadowing** – les droits affectés à ce groupe sont responsables des actions enregistrées dans le journal de réplication.

  - **Write** – permet la replication de toutes les données écrites par l'utilisateur. Ne s'applique qu'aux périphériques de type DVD/CD-ROM, Floppy, iPhone, Parallel port, Removable, Serial port, Windows Mobile et Palm.
  - **Print** – permet la réplication de tous les documents envoyés à des imprimantes. Par la suite, ces documents peuvent être affichés à l'aide de DeviceLock Printer Viewer. Ne s'applique qu'aux périphériques de type Printer.
  - **Write Non-files** – permet la réplication de tous les objets autres que des fichiers (Calendrier, Contacts, Tâches, etc.) écrits par l'utilisateur. Ne s'applique qu'aux périphériques de type iPhone, Windows Mobile et Palm.

Dans la table suivante, vous pouvez voir les droits de types d'audit susceptibles d'être assignés aux différents types de dispositifs et ce qui est inscrit dans le journal. Pour tous les événements, DeviceLock Service enregistre le type d'événement, la date et l'heure, le type de périphérique, le nom d'utilisateur et les renseignements sur le processus en plus des informations spécifiques à l'événement conformément aux indications ci-dessous.

TYPE DE PERIPHERIQUE	DROITS
BlackBerry	• Audit: Read **+** *L'action Device Access est enregistrée dans le journal d'audit.* • Audit: Write/Print **+** *L'action Device Access est enregistrée dans le journal d'audit*. • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
Bluetooth	• Audit: Read **+** *L'action Device Access est enregistrée dans le journal.* • Audit: Write/Print **+** *L'action Device Access est enregistrée dans le journal*. • Audit: Execute **-**

TYPE DE PERIPHERIQUE	DROITS
	• Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
Clipboard	• Audit: Read **-** • Audit: Write/Print **-** • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **+** *Les actions Copy Text, Copy File, Copy Image, Copy Audio, Copy Unidentified et Screenshot sont inscrites dans le journal d'audit*. • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
DVD/CD-ROM	• Audit: Read **+** *Les actions Open, Device Access, Direct Access et Eject, les noms de fichiers et les options (Read, DirectRead, Eject, DirList) sont enregistrés dans le journal d'audit*. • Audit: Write/Print **+** *Les actions Open, Device Access et Direct Access et les options (Write, Del, DirectWrite) sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **+** *Les images de CD/DVD au format CUE et/ou les fichiers sont enregistrés dans le journal de réplication.* • Shadowing: Write Non-files **-**
FireWire port	• Audit: Read **+** *Les actions Insert, Remove et Device Access et les noms de périphérique sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Insert, Remove et Device Access et les noms de périphérique sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**

TYPE DE PERIPHERIQUE	DROITS
Floppy	• Audit: Read **+** *Les actions Open, Mount, Unmount et Direct Access, les noms de fichiers et les options (Read, DirectRead, Eject, DirList) sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename et Create new, les noms de fichiers et les options (Write, Del, DirectWrite, Format, DirCreate) sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **+** *Les fichiers sont enregistrés dans le journal de réplication*. • Shadowing: Write Non-files **-**
Hard disk	• Audit: Read **+** *Les actions Open, Mount, Unmount et Direct Access, les noms de fichiers et les options (Read, DirectRead, Eject, DirList) sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename et Create new, les noms de fichiers et les options (Write, Del, DirectWrite, Format, DirCreate) sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
Infrared port	• Audit: Read **+** *L'action Device Access est enregistrée dans le journal d'audit.* • Audit: Write/Print **+** *L'action Device Access est enregistrée dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**

TYPE DE PERIPHERIQUE	DROITS
iPhone	• Audit: Read **+** *L'action Read File et les noms de fichiers sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Write File, Rename File et Delete File, ainsi que les noms de fichiers sont enregistrés dans le journal d'audit.* • Audit: Execute **–** • Audit: Read Non-files **+** *Les actions Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Backup, Read Note et Read Media, ainsi que les noms d'objets sont enregistrés dans le journal d'audit*. • Audit: Write Non-files **+** *Les actions Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-mail, Write Backup, Write Note, Delete Note, Write Media, Rename Media and Delete Media, ainsi que les noms d'objets sont enregistrés dans le journal d'audit*. • Audit: Copy **-** • Shadowing: Write/Print **+** *Les fichiers sont enregistrés dans le journal de réplication*. • Shadowing: Write Non-files **+** *Toutes les données contenant des objets autres que des fichiers (Calendrier, Contacts, Tâches, etc.) doivent être enregistrées dans le journal de réplication*.
Palm	• Audit: Read **+** *L'action Read File, les noms de fichiers et la case Sync sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *L'action Write File, les noms de fichiers et la case Sync sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **+** *Les actions et noms d'objets Read Calendar, Read Contact, Read Expense, Read E-mail, Read Document, Read Memo, Read Notepad, Read Task et Read Media Sont enregistrés dans le journal d'audit.* • Audit: Write Non-files **+** *Les actions et les noms d'objets Write Calendar, Write Contact, Write Expense, Write E-mail, Write Document, Write Memo, Write Notepad, Write Task, Write Media et Install Sont enregistrés dans le journal d'audit*. • Audit: Copy **-** • Shadowing: Write/Print **+** *Les fichiers sont enregistrés dans le journal de réplication*. • Shadowing: Write Non-files **+** *Toutes les données contenues dans les objets autres que des fichiers (Calendar, Contacts, Tasks, etc.) doivent être enregistrées dans le journal de réplication.*

TYPE DE PERIPHERIQUE	DROITS
Parallel port	• Audit: Read **+** *L'action Device Access est enregistrée dans le journal d'audit*. • Audit: Write/Print **+** *L'action Device Access est enregistrée dans le journal d'audit*. • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **+** *Toutes les données envoyées au port sont enregistrées dans le journal de réplication.* • Shadowing: Write Non-files **-**
Printer	• Audit: Read **-** • Audit: Write/Print **+** *L'action Print, les noms de documents et d'imprimantes sont enregistrés dans le journal d'audit*. • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **-** • Audit: Copy **-** • Shadowing: Write/Print **+** *Toutes les données envoyées à l'imprimante sont enregistrées dans le journal de réplication au format natif du spooler d'imprimante.* • Shadowing: Write Non-files **-**
Removable	• Audit: Read **+** *Les actions Open, Mount, Unmount et Direct Access, les noms de fichiers et les options (Read, DirectRead, Eject, DirList) sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename et Create new, les noms de fichiers et les options (Write, Del, DirectWrite, Format, DirCreate) sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **+** *Les fichiers sont enregistrés dans le journal de réplication*. • Shadowing: Write Non-files **-**

TYPE DE PERIPHERIQUE	DROITS
Serial port	• Audit: Read **+** *Les actions Mount, Unmount, Insert, Remove et Device Access sont enregistrées dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Mount, Unmount, Insert, Remove et Device Access sont enregistrées dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **+** *Toutes les données envoyées au port sont enregistrées dans le journal de réplication.* • Shadowing: Write Non-files **-**
Tape	• Audit: Read **+** *Les événements Open, Device Access et Direct Access et les options (Read, DirectRead) sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les événements Open, Device Access et Direct Access et les options (Write, DirectWrite) sont enregistrés dans le journal d'audit*. • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
USB port	• Audit: Read **+** *Les actions Insert, Remove et Device Access et les noms de périphérique sont enregistrés dans le journal d'audit.* • Audit: Write/Print **+** *Les actions Insert, Remove et Device Access et les noms de périphérique sont enregistrés dans le journal d'audit.* • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**

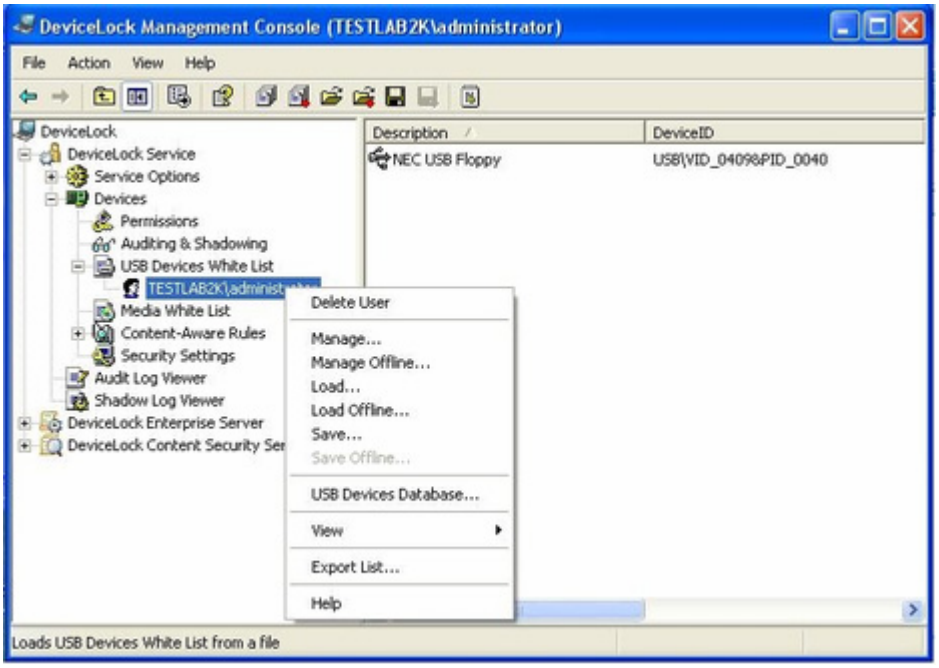
TYPE DE PERIPHERIQUE	DROITS
WiFi	• Audit: Read **+** *L'action Device Access est enregistrée dans le journal d'audit*. • Audit: Write/Print **+** *L'action Device Access est enregistrée dans le journal d'audit*. • Audit: Execute **-** • Audit: Read Non-files **-** • Audit: Write Non-files **–** • Audit: Copy **-** • Shadowing: Write/Print **-** • Shadowing: Write Non-files **-**
Windows Mobile	• Audit: Read **+** *Les actions Read File, Get File Attributes, Create New File, Overwrite/Create File, Open File et Open/Create File, ainsi que les noms et les codes de fichiers figurent dans le journal d'audit*. • Audit: Write/Print **+** *Les actions Write File, Delete File, Rename File, Create File, Create New File, Overwrite/Create File, Open File, Open/Create File, Overwrite, Set File Attributes, Create Shortcut et Copy File, ainsi que les noms et les codes de fichiers figurent dans le journal d'audit.* • Audit: Execute **+** *Les actions Invoke et Execute, les noms de fichiers et de fonctions (procédures) figurent dans le journal d'audit*. • Audit: Read Non-files **+** *Les actions Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Attachment, Read Note, Read Task, Read Media, Read Pocket Access et Read Unknown, ainsi que les noms d'objets figurant dans le journal d'audit.* • Audit: Write Non-files **+** *Les actions Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-Mail, Write Attachment, Delete Attachment, Write Note, Delete Note, Write Task, Delete Task, Write Media, Delete Media, Write Pocket Access, Delete Pocket Access, Write Unknown et Delete Unknown, ainsi que les noms d'objets figurant dans le journal d'audit*. • Audit: Copy **-** • Shadowing: Write/Print **+** *Les fichiers figurnet dans le journal de réplication*. • Shadowing: Write Non-files **+** *Toutes les données contenant des objets autres que des fichiers (Calendar, Contacts, Tasks, etc.) doivent être enregistrées dans le journal de réplication*.

Remarque: Tant que **Audit Allowed** ou **Audit Denied** n'est pas coché pour ce type de matériel, l'enregistrement dans le journal d'audit est désactivé pour ce matériel, malgré les règles d'audits définies.

L'enregistrement n'est possible ni pour les périphériques répertoriés dans la white list, ni pour la classe entière de périphériques si le contrôle d'accès de cette classe a été bloqué dans les **Security Settings**.

USB Devices White List (Liste blanche de périphériques USB) (Regular Profile)

La liste blanche des périphériques permet d'établir une liste de périphériques qui ne doivent jamais être verrouillés par le système, quelle qu'en soit la configuration. Le but est de pouvoir autoriser certains périphériques particuliers tout en verrouillant tous les autres.



Les périphériques figurant dans la liste blanche peuvent être définis individuellement pour tous les utilisateurs et les groupes. Pour plus d'informations sur la façon dont fonctionne la liste blanche des périphériques, veuillez vous reporter au chapitre Contrôle d'accès géré de ce manuel.

Remarque: Aucun audit n'est effectué des tentatives d'accès à un périphérique figurant dans la liste blanche de la part des utilisateurs, contrairement aux tentatives d'insertion ou de suppression de ce genre de périphériques qui font, elles, l'objet d'un audit.

L'identification des périphériques dans la liste blanche s'effectue de deux façons différentes:

- **Par modèle de périphérique**: contient tous les périphériques du même modèle. Chaque périphérique est identifié par une combinaison de Vendor Id (VID) et de Product Id (PID).

  Cette combinaison de VID et de PID décrit un modèle de périphérique individuel mais pas un périphérique individuel. Cela signifie que tous les périphériques correspondant au modèle et au vendeur considérés passeront pour des périphériques autorisés.

- **Par périphérique**: ne contient qu'un seul périphérique. Chaque périphérique est identifié par une combinaison de Vendor Id (VID), de Product Id (PID) et de Serial Number (SN).

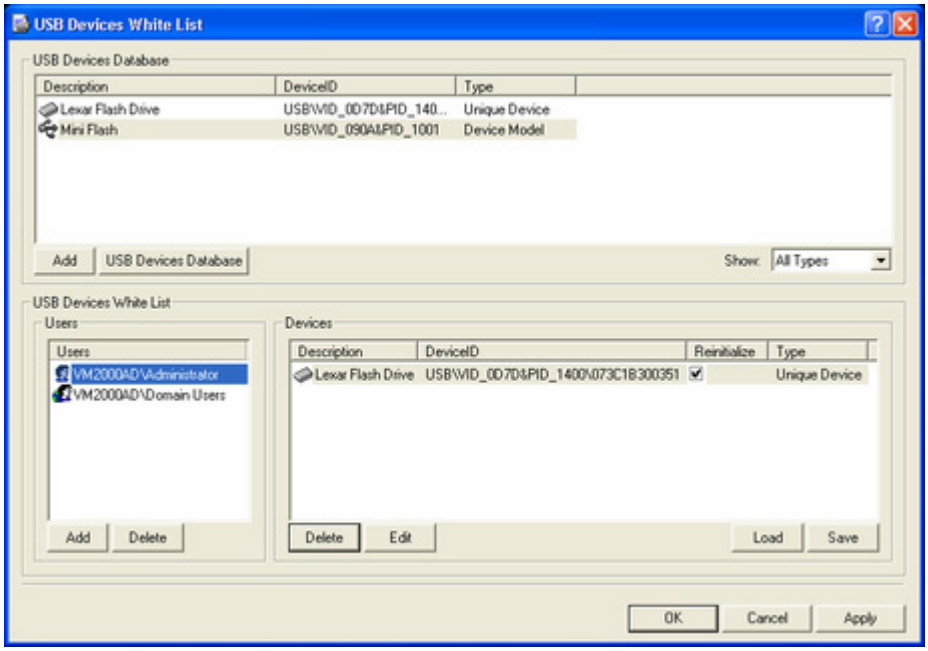
Tous les périphériques ne possèdent pas un numéro de série. Un périphérique ne peut être ajouté à la liste blanche en tant que périphérique individuel que si son fabricant lui a attribué un numéro de série en phase de production.

Deux actions sont requises pour autoriser l'accès à un périphérique:

1. Ajouter le périphérique dans la base de données des périphériques, ce qui permet de l'ajouter à la liste blanche.
2. Ajouter le périphérique à la liste blanche de l'utilisateur ou du groupe spécifié. Ce périphérique est alors considéré comme «autorisé», ce qui permet à l'utilisateur ou au groupe d'y accéder au niveau de l'interface (USB).

Remarque: Vous pouvez définir des listes blanches de périphériques USB différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. La liste blanche de périphériques USB en ligne (Regular Profile) s'applique aux ordinateurs client qui fonctionnent en ligne. La liste blanche de périphériques USB hors ligne (Offline Profile) s'applique aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition de la liste blanche de périphériques USB hors ligne, reportez-vous au chapitre intitulé «Gestion de la liste blanche de périphériques USB hors ligne.»

Pour définir la liste blanche, sélectionnez **Manage** à l'aide du menu contextuel disponible en cliquant droit. Vous pouvez aussi utiliser le bouton approprié sur la barre d'outils.



Dans la liste **USB Devices Database** située dans la partie supérieure de la boîte de dialogue, vous pouvez voir les périphériques qui ont été ajoutés à la base de données.

Une fois les périphériques de la base de données ajoutés à la liste blanche d'un utilisateur déterminé, ils se convertissent en matériels autorisés pour lesquels le contrôle d'accès est désactivé lorsque cet utilisateur est connecté.

Vous pouvez ajouter un matériel à la liste blanche des périphériques USB en deux étapes:

1. Sélectionnez l'utilisateur ou le groupe d'utilisateurs pour lequel ce matériel doit être autorisé.

   Cliquez sur le bouton **Add** dans la liste Users pour ajouter l'utilisateur ou le groupe considéré. Pour supprimer une entrée de la liste **Users**, utilisez le bouton **Delete**.

2. Sélectionnez les données de matériel appropriées dans la liste **USB Devices Database** et appuyez sur le bouton **Add**.

   Si le périphérique possède un numéro de série, il peut être ajouté deux fois à la liste blanche: en tant que Type de périphérique et en tant que Périphérique individuel. Dans ce cas, le Type de périphérique prévaut sur le Périphérique individuel.

Lorsque la case **Control as Type** est cochée, le contrôle d'accès aux périphériques de la liste blanche est désactivé au niveau de l'interface (USB). Si le périphérique affiché dans la liste blanche (p.ex. la clé USB) appartient aux deux niveaux: interface (USB) et typologique (amovible), les autorisations (le cas échéant) pour le niveau typologique seront de toutes façons appliquées.

Dans les autres cas, si la case **Control as Type** est cochée, le contrôle d'accès au niveau du type est également désactivé. Par exemple, en décochant la case **Control as Type** pour le lecteur flash USB, vous pouvez contourner les contrôles de sécurité au niveau Removable.

Remarque: Lorsque vous ajoutez un périphérique composite USB (autrement dit, un périphérique qui est représenté dans le système par un périphérique composite parent et un ou plusieurs périphériques d'interface enfants) à la liste blanche des périphériques USB, tenez compte des points suivants:

Si vous ajoutez l'un ou l'autre des périphériques d'un périphérique composite USB à la liste blanche, le contrôle d'accès sera désactivé pour tous les périphériques du périphérique composite au niveau de l'interface (port USB). Si le périphérique répertorié dans la liste blanche appartient aux deux niveaux: interface (USB) et type (amovible, par exemple), et si la case **Control as Type** est cochée, les autorisations (éventuelles) pour le niveau de type seront de toutes façons appliquées.

S'il s'avère nécessaire d'obliger le périphérique répertorié dans la liste blanche à se réinitialiser (rebrancher) lorsque le nouvel utilisateur est connecté, cochez la case **Reinitialize**.

Certains périphériques USB (comme la souris) ne fonctionneront pas sans réinitialisation. Il est donc conseillé de cocher cette case pour les périphériques autres que les dispositifs de stockage.

Il est recommandé de ne pas cocher la case **Reinitialize** pour les dispositifs de stockage (tels que les clés USB, les CD/DVD-ROM, les disques durs externes et ainsi de suite).

Certains périphériques, dont les pilotes n'acceptent pas la réinitialisation logicielle, ne peuvent pas être réinitialisés à partir de DeviceLock Service. Si un tel périphérique a été ajouté à la liste blanche mais ne fonctionne pas, l'utilisateur devra le débrancher et le rebrancher manuellement pour redémarrer le pilote du périphérique.

Pour éditer la description d'un appareil, sélectionnez l'élément approprié à partir de l'**USB Devices White List**, puis cliquez sur **Edit**. Cliquez sur **Delete** pour supprimer l'article de l'appareil sélectionné (utilisez Ctrl et/ou Maj pour sélectionner simultanément plusieurs appareils).

Pour enregistrer la liste blanche sur un fichier externe, appuyez sur le bouton **Save**, puis sélectionnez le nom du fichier. Pour charger une liste blanche préalablement enregistrée, appuyez sur le bouton **Load** et sélectionnez un fichier qui contient la liste des terminaux.

Pour gérer la base de données de périphériques, vous pouvez cliquer sur **USB Devices Database** et ouvrir la boîte de dialogue correspondante.

Remarque: Si vous ajoutez un iPhone à la liste blanche de périphériques USB, le contrôle d'accès sera désactivé tant pour l'iPhone que pour son appareil photo au niveau de l'interface (port USB). Par conséquent, vous ne pourrez pas autoriser l'accès à l'iPhone et refuser l'accès à son appareil photo au niveau de l'interface (port USB). Dans la base de périphériques USB, un périphérique iPhone figure en tant que «Apple Mobile Device USB Driver».

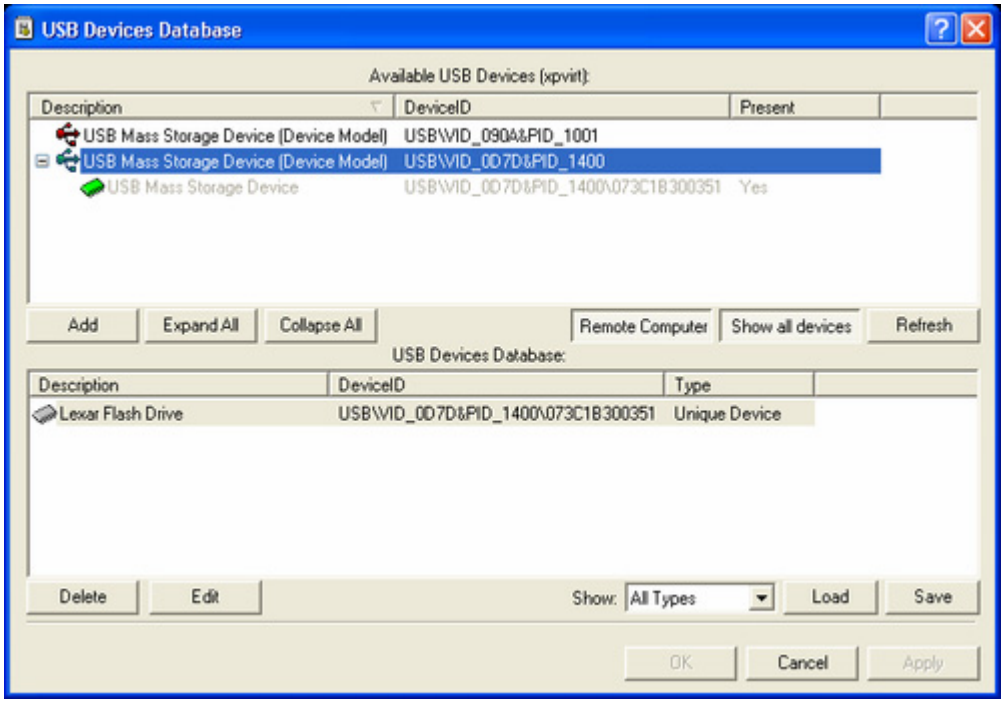
Cependant, il est possible d'autoriser l'accès à l'appareil photo de l'iPhone et de refuser l'accès à l'iPhone. Pour ce faire, vous pouvez utiliser l'une ou l'autre des méthodes suivantes :

Méthode 1. Pour autoriser l'accès à l'appareil photo de l'iPhone, ajoutez l'iPhone à la liste blanche des périphériques USB et cochez la case **Control as Type**. Pour refuser l'accès à l'iPhone, choisissez l'option No Access pour les périphériques de type **iPhone**.

Méthode 2. Pour autoriser l'accès à l'appareil photo de l'iPhone, décochez la case **Access control for USB scanners and still image devices** dans les **Security Settings**. Pour refuser l'accès à l'iPhone, choisissez l'option No Access pour les périphériques de type **USB port**.

USB Devices Database (Base de périphériques USB)

La boîte de dialogue **USB Devices Database** permet d'ajouter de nouveaux périphériques à la base de données et à éditer les périphériques existants.



Avant qu'un périphérique ne puisse être autorisé dans la White List, il doit être ajouté à la base de données.

La liste des **Available USB Devices** située dans la partie supérieure de la boîte de dialogue contient tous les périphériques disponibles sur l'ordinateur.

Les périphériques sont affichés sous forme d'arborescence simple, dans laquelle l'élément parent représente le **modèle de périphérique** et l'élément enfant représente le **périphérique individuel**. Si aucun **périphérique individuel** n'apparaît, c'est que le périphérique correspondant ne possède pas de numéro de série.

Cette liste affiche, soit tous les périphériques branchés au moment considéré (si **Show all devices** n'apparaît pas en surbrillance), soit tous les périphériques qui ont déjà été branchés sur le port de cet ordinateur (si **Show all devices** apparaît en surbrillance).

La liste des périphériques disponibles est automatiquement mise à jour et elle affiche immédiatement les nouveaux périphériques. Pour mettre à jour la liste manuellement, cliquez sur **Refresh**.

Pour récupérer les périphériques d'un ordinateur distant, appuyez sur le bouton **Remote Computer**. Ce bouton est indisponible lorsque vous êtes connecté à l'ordinateur local.

Dans la liste **USB Devices Database** située en bas de la boîte de dialogue, vous pouvez voir les périphériques qui figurent déjà dans la base de données.

Pour ajouter de nouveaux périphériques à cette liste, sélectionnez leurs noms dans la liste **Available USB Devices** et cliquez sur **Add**. Si le périphérique que vous venez de sélectionner figure déjà dans la base de données, il ne peut pas être ajouté à nouveau.

Pour éditer la description d'un périphérique, sélectionnez-le dans la liste **USB Devices Database** et cliquez sur **Edit**.

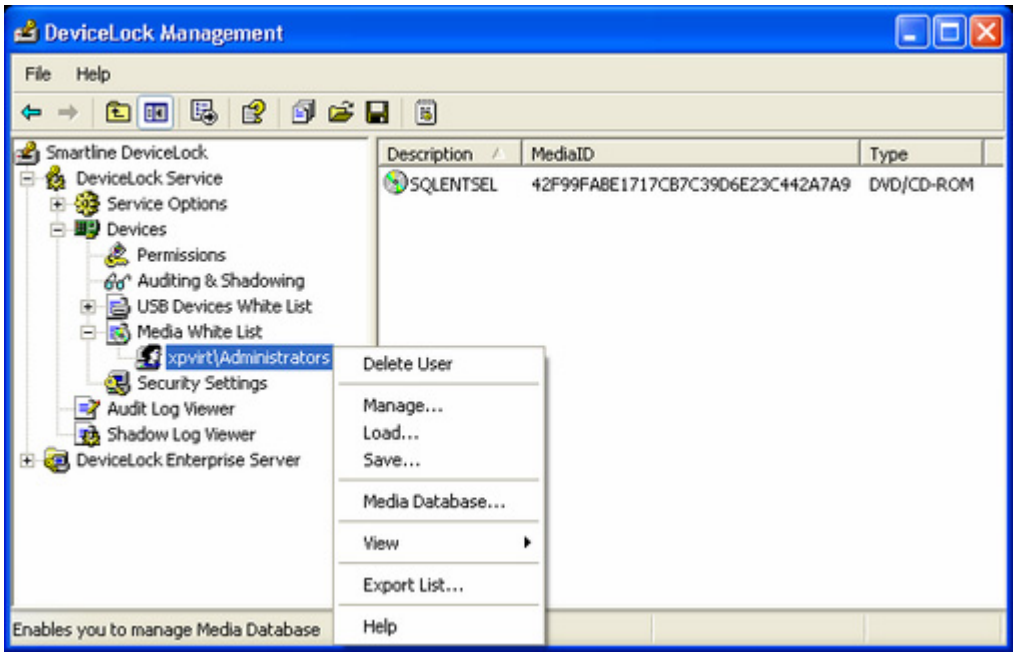
Cliquez sur **Delete** pour supprimer l'article de l'appareil sélectionné (utilisez Ctrl et/ou Maj pour sélectionner simultanément plusieurs appareils).

Il est aussi possible de sauvegarder une base de données en créant un fichier de sauvegarde externe. Pour ce faire, cliquez sur **Save**, puis sélectionnez un format pour le fichier à créer — .txt ou .csv.

Les bases de données ainsi sauvegardées peuvent être chargées en cliquant sur **Load** et en sélectionnant le fichier souhaité.

Media White List (Liste blanche de médias) (Regular Profile)

La liste blanche de médias permet l'identification individuelle d'un CD-ROM/DVD spécifique par son empreinte digitale et permet d'y accéder en lecture, même si DeviceLock Service bloque les lecteurs CD-ROM/DVD.



On peut configurer la liste blanche de médias afin de permettre à certains utilisateurs et groupes l'accès à une bibliothèque de disques DVD/CD-ROM approuvés; ainsi, seuls les utilisateurs autorisés peuvent utiliser les informations approuvées.

Tout changement du contenu du média changera l'empreinte digitale, ce qui invalidera l'autorisation. Si l'utilisateur copie le média sans aucune modification (copie octet-à-octet), cette copie sera acceptée comme étant le média autorisé.

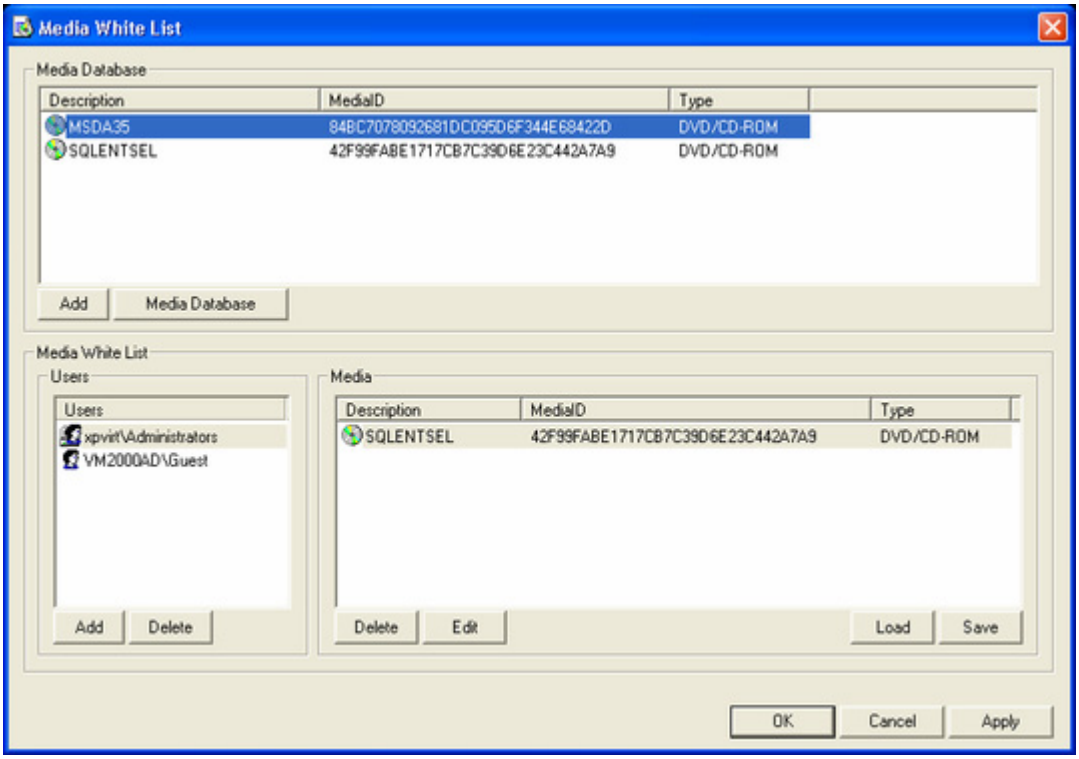
Remarque: L'accès aux médias de la liste blanche ne peut être accordé qu'au niveau du type (DVD/CD-ROM). Si le lecteur DVD/CD est branché sur un port USB ou FireWire, et si l'accès à ce port est interdit, l'accès au média de la liste blanche sera aussi interdit.

Deux actions sont requises pour autoriser l'accès à un média:

1. Ajouter le média dans la base de données des médias, ce qui permet de l'ajouter à la liste blanche.
2. Ajouter le média à la liste blanche de l'utilisateur ou du groupe spécifié. Ce média est alors considéré comme «autorisé», ce qui permet à l'utilisateur ou au groupe d'y accéder au niveau du type (DVD/CD-ROM).

Remarque: Vous pouvez définir des listes blanches de médias différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. La liste blanche de médias en ligne (Regular Profile) s'applique aux ordinateurs client qui fonctionnent en ligne. La liste blanche de médias hors ligne (Offline Profile) s'applique aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition de la liste blanche de médias hors ligne, reportez-vous au chapitre intitulé «Gestion de la liste blanche de médias hors ligne.»

Pour définir la liste blanche des médias, sélectionnez **Manage** à l'aide du menu contextuel disponible en cliquant droit. Vous pouvez aussi utiliser le bouton approprié dans la barre d'outils.



La liste **Media Database** située dans la partie supérieure de la boîte de dialogue contient tous les médias précédemment ajoutés à la base de données.

Une fois les médias de la base de données ajoutés à la liste blanche d'un utilisateur déterminé, ils se convertissent en médias autorisés pour lesquels le contrôle d'accès est désactivé lorsque cet utilisateur est connecté.

Vous pouvez ajouter un média à la liste blanche de médias en deux étapes:

1. Sélectionnez l'utilisateur ou le groupe d'utilisateurs pour lequel ce média doit être autorisé.

   Cliquez sur le bouton **Add** dans la liste **Users** pour ajouter l'utilisateur ou le groupe considéré. Pour supprimer une entrée de la liste **Users**, utilisez le bouton **Delete**.
2. Sélectionnez les données de média appropriées dans la liste **Media Database** et appuyez sur le bouton **Add**.

Pour éditer la description d'un média, sélectionnez l'élément approprié à partir de la **Media White List** puis cliquez sur **Edit**.

Cliquez sur **Delete** pour supprimer l'article du média sélectionné (utilisez Ctrl et/ou Maj pour sélectionner simultanément plusieurs articles).

Pour enregistrer la liste blanche de média sur un fichier externe, appuyez sur le bouton **Save**, puis sélectionnez le nom du fichier.

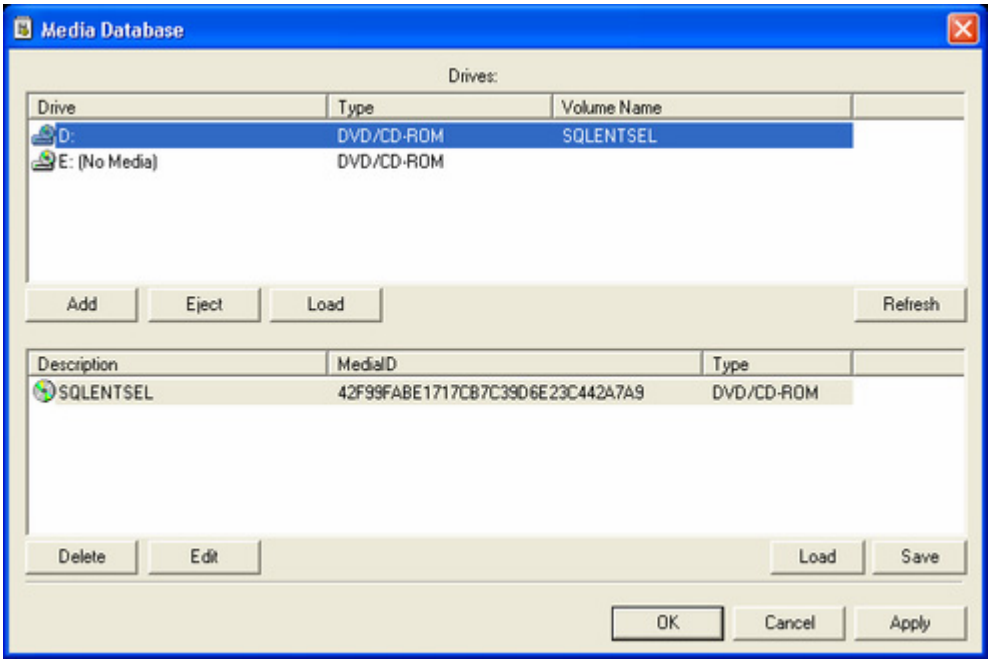
Pour charger une liste blanche préalablement enregistrée, appuyez sur le bouton **Load** et sélectionnez un fichier contenant la liste des médias.

Pour gérer la base de données de médias, vous pouvez cliquer sur **Media Database** et ouvrir la boîte de dialogue correspondante.

Remarque: La liste blanche de médias ne permet que l'accès en lecture aux médias autorisés. Il est impossible d'autoriser l'écriture.

Media Database (Base de données des médias)

La boîte de dialogue **Media Database** sert à ajouter de nouveaux médias à la base de données et à éditer les médias existants.



Avant qu'un média ne puisse être autorisé par la White List, il doit être ajouté à la base de données.

La liste **Drives** située dans la partie supérieure de la boîte de dialogue contient tous les lecteurs susceptibles de contenir des médias disponibles sur l'ordinateur.

La liste est automatiquement mise à jour et elle affiche immédiatement les nouveaux médias. Pour mettre à jour la liste manuellement, cliquez sur **Refresh**.

Dans la liste située en bas de la boîte de dialogue, vous pouvez voir les médias qui figurent déjà dans la base de données.

Pour ajouter de nouveaux médias à cette liste, sélectionnez leurs noms dans la liste **Drives** et cliquez sur **Add**. L'ordinateur peut mettre un certain temps (selon la taille du média) pour autoriser le média. Si le média que vous venez de sélectionner figure déjà dans la base de données, il ne peut être ajouté à nouveau.

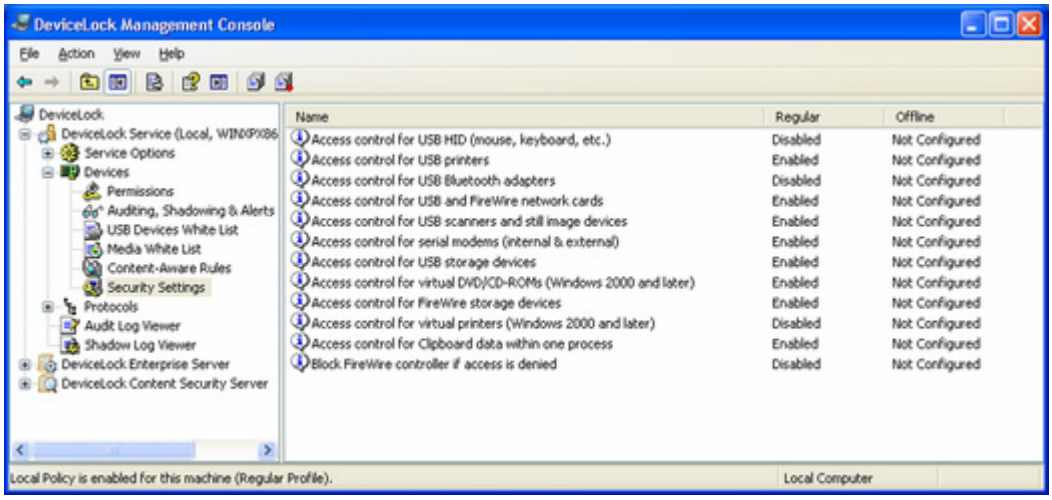
Pour éditer la description d'un média, sélectionnez l'élément approprié dans la liste puis cliquez sur **Edit**.

Cliquez sur **Delete** pour supprimer un article sélectionné (utilisez Ctrl et/ou Maj pour sélectionner simultanément plusieurs articles).

Il est aussi possible de sauvegarder une base de données en créant un fichier de sauvegarde externe. Pour ce faire, cliquez sur **Save**, puis sélectionnez un format pour le fichier à créer — .txt ou .csv. Les bases de données ainsi sauvegardées peuvent être chargées en cliquant sur **Load** et en sélectionnant le fichier souhaité.

Security Settings (Paramètres de sécurité) (Regular Profile)

Il existe une liste de paramètres additionnels de sécurité qui s'appliquent aux autorisations et aux règles d'audit pour certains types de périphérique.


DeviceLock Management Console
File Action View Help
DeviceLock
DeviceLock Service (Local, WIN0PX86)
Service Options
Devices
Permissions
Auditing, Shadowing & Alerts
USB Devices White List
Media White List
Content-Aware Rules
Security Settings
Protocols
Audit Log Viewer
Shadow Log Viewer
DeviceLock Enterprise Server
DeviceLock Content Security Server
Name
Regular
Offline
Access control for USB HID (mouse, keyboard, etc.) Disabled Not Configured
Access control for USB printers Enabled Not Configured
Access control for USB Bluetooth adapters Disabled Not Configured
Access control for USB and FireWire network cards Enabled Not Configured
Access control for USB scanners and still image devices Enabled Not Configured
Access control for serial modems (internal & external) Enabled Not Configured
Access control for USB storage devices Enabled Not Configured
Access control for virtual DVD/CD-ROMs (Windows 2000 and later) Enabled Not Configured
Access control for FireWire storage devices Enabled Not Configured
Access control for virtual printers (Windows 2000 and later) Disabled Not Configured
Access control for Clipboard data within one process Enabled Not Configured
Block FireWire controller if access is denied Disabled Not Configured
Local Policy is enabled for this machine (Regular Profile).
Local Computer

Ces paramètres de sécurité permettent de verrouiller entièrement certains types de périphériques, tout en autorisant certaines classes de périphériques sans avoir à autoriser chaque périphérique dans la liste blanche.

Par exemple, vous pouvez empêcher l'utilisation de tous les périphériques USB, sauf la souris et le clavier.

DeviceLock accepte les paramètres additionnels de sécurité suivants:

- **Access control for USB HID**: permet l'audit et le contrôle d'accès à des périphériques d'entrée utilisateur (souris, clavier, etc.) branchés sur un port USB. Toutefois, même si le port USB est verrouillé, les périphériques d'entrée utilisateurs continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques si cette case est décochée.
- **Access control for USB printers**: permet l'audit et le contrôle d'accès aux imprimantes branchées sur un port USB. Toutefois, même si le port USB est verrouillé, les imprimantes continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques si cette case est décochée.
- **Access control for USB scanners and still image devices**: permet l'audit et le contrôle d'accès aux scanners et périphériques de traitement d'images fixes branchés sur un port USB. Toutefois, même si le port USB est verrouillé, ces périphériques continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques si cette case est décochée.
- **Access control for USB Bluetooth adapters**: permet l'audit et le contrôle d'accès aux adaptateurs Bluetooth branchés sur un port USB. Toutefois, même si le port USB est verrouillé, les adaptateurs Bluetooth continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques.

Ce paramètre n'affecte l'audit et le contrôle d'accès qu'au niveau de l'interface (USB). Si le périphérique appartient aux deux niveaux, les autorisations et règles d'audit (le cas échéant) pour le niveau typologique (Bluetooth) seront de toute façon appliquées.

- **Access control for USB storage devices**: permet l'audit et le contrôle d'accès aux périphériques de stockage (tels que les lecteurs flash) branchés sur un port USB. Toutefois, même si le port USB est verrouillé, les périphériques de stockage continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques.

  Ce paramètre n'affecte l'audit et le contrôle d'accès qu'au niveau de l'interface (USB). Si le périphérique appartient aux deux niveaux (interface et typologique), les autorisations et les règles d'audit (le cas échéant) pour le niveau typologique (Amovible, Disquette, DVD/CD-ROM ou Disque Dur) seront de toutes façon appliquées.

- **Access control for USB and FireWire network cards**: permet l'audit et le contrôle d'accès aux cartes réseau branchées sur un port USB ou FireWire (IEEE 1394). Toutefois, même si le port USB ou FireWire est verrouillé, les cartes réseau continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques.
- **Access control for FireWire storage devices**: cochez cette case pour permettre à DeviceLock Service d'auditer et de contrôler l'accès aux périphériques de stockage branchés sur le port FireWire. Toutefois, même si le port FireWire est verrouillé, les périphériques de stockage continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques.

  Ce paramètre n'affecte l'audit et le contrôle d'accès qu'au niveau de l'interface (FireWire). Si le périphérique appartient aux deux niveaux (interface et typologique), les autorisations et les règles d'audit (le cas échéant) pour le niveau typologique (Amovible, Disquette, DVD/CD-ROM ou Disque Dur) seront de toutes façon appliquées.

- **Access control for serial modems (internal & external)**: permet l'audit et le contrôle d'accès aux modems branchés dans le port COM. Toutefois, même si le port COM est verrouillé, les modems continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques.
- **Access control for virtual CD-ROMs**: en cochant cette option, vous autorisez DeviceLock Service à auditer et à contrôler l'accès aux CD-ROM virtuels (émulés par voie logicielle). Toutefois, même si le périphérique CD-ROM est verrouillé, les lecteurs virtuels continuent à fonctionner normalement et aucun audit n'est effectué de ces périphériques. Cette fonctionnalité n'est disponible que sur Windows 2000 et les systèmes d'exploitation suivants.
- **Access control for virtual printers**: Si cette option est activée, DeviceLock peut surveiller et contrôler l'accès aux imprimantes virtuelles qui n'envoient pas les documents à des périphériques réels, mais les impriment dans des fichiers (p.ex. des convertisseurs PDF). Sinon, même si l'imprimante physique est verrouillée, les imprimantes virtuelles continuent à imprimer normalement et aucun audit n'a lieu

pour ces périphériques. Cette fonctionnalité n'est disponible que sur les systèmes d'exploitation Windows 2000 et postérieurs.

- **Access control for inter-application copy/paste clipboard operations**: Activez cette option pour autoriser DeviceLock Service à auditer et à contrôler l'accès aux opérations de copier/coller entre différentes applications. À défaut, le contrôle d'accès aux opérations de copier/coller entre différentes applications sera désactivé, même si ce dernier est verrouillé, et aucun audit ne sera effectué pour ces opérations.
- **Block FireWire controller if access is denied**: permet de désactiver les contrôleurs FireWire lorsque le compte Tous ne possède pas les permissions d'accès pour le type de périphérique port FireWire.

Remarque: Vous pouvez définir des paramètres de sécurité différents selon qu'ils s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les paramètres de sécurité en ligne (Regular Profile) s'appliquent aux ordinateurs client qui fonctionnent en ligne. Les paramètres de sécurité hors ligne (Offline Profile) s'appliquent aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des paramètres de sécurité hors ligne, reportez-vous au chapitre intitulé «Gestion des paramètres de sécurité hors ligne.»

Pour modifier ces paramètres de sécurité, double-cliquez sur l'entrée du paramètre pour basculer d'un état à l'autre (activé/désactivé) Vous pouvez aussi sélectionner l'élément **Manage** du menu contextuel disponible en cliquant droit, ou utiliser le bouton approprié sur la barre d'outils.

Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual DVD/CD-ROMs (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
Access control for Clipboard data within one process
Block FireWire controller if access is denied
OK
Cancel

Les Paramètres de Sécurité (Security Settings) sont similaires à ceux de la Devices White List, à trois exceptions majeures près:

1. L'utilisation des Paramètres de sécurité permet uniquement d'autoriser une classe entière de périphériques. Elle ne permet pas l'utilisation exclusive d'un modèle spécifique d'une classe de périphériques par ailleurs non-autorisée.

Par exemple, si vous désactivez **Access control for USB storage devices**, vous donnez l'autorisation d'utiliser tous les périphériques de stockages USB, quels qu'en soient les modèles et les fournisseurs. Par contre, en faisant figurer un modèle particulier de clés USB qui vous intéresse dans la liste blanche des périphériques, vous pouvez continuer à l'utiliser tout en sachant qu'aucun autre matériel de cette classe de périphériques ne pourra être utilisé.

2. L'utilisation des Paramètres de sécurité ne permet d'effectuer des sélections qu'à partir de classes de périphériques prédéfinies. Si le périphérique qui vous intéresse n'appartient pas à l'une des classes prédéfinies, les règles de sécurité ne peuvent pas être appliquées.

   Par exemple, il n'existe pas aujourd'hui de classe spécifique pour les lecteurs smart card dans les règles de sécurité. Pour permettre l'accès à un lecteur smart card lorsque le port est verrouillé, vous devez donc faire appel à la liste blanche des périphériques.

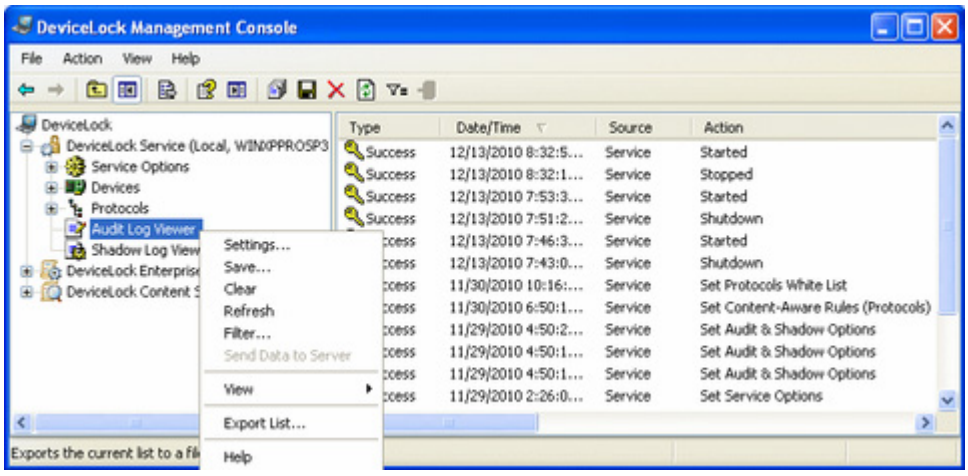
3. Les paramètres de sécurité ne peuvent pas être définis utilisateur par utilisateur, ils affectent tous les utilisateurs de l'ordinateur local. Cependant, les terminaux de la liste blanche peuvent être définis individuellement pour tous les utilisateurs et les groupes.

Remarque: Les paramètres de sécurité ne fonctionnent que pour les périphériques qui emploient les pilotes standards de Windows. Certains périphériques utilisent des pilotes propriétaires et leurs classes ne peuvent pas être reconnues par DeviceLock Service. Par conséquent, le contrôle d'accès à de tels périphériques ne peut être désactivé par les paramètres de sécurité. Dans ce cas, vous pouvez utiliser la Device White List pour autoriser de tels périphériques manuellement.

Audit Log Viewer (Service)

Il existe un visionneur du journal d'audit permettant de récupérer les données du journal d'audit de DeviceLock à partir du sous-système de journalisation des événements Windows de l'ordinateur local.

Le sous-système de journalisation des événements Windows n'est utilisé pour stocker les données d'audit que si l'option **Event Log** ou **Event & DeviceLock Logs** est sélectionnée dans le paramètre **Audit log type** des Service Options. Sinon, les données d'audit sont stockées dans le journal propriétaire et peuvent être affichées à l'aide de l'Audit Log Viewer du serveur.



Le journal d'audit sert à enregistrer les événements générés par les actions d'un utilisateur en relation avec un périphérique et soumises aux règles d'audit. Pour plus d'informations, veuillez lire le chapitre Auditing & Shadowing de ce manuel.

Les modifications de la configuration de DeviceLock Service génèrent aussi des événements dans le journal d'audit si la case appropriée est cochée dans les Service Options.

Les colonnes de ce visionneur sont les suivantes:

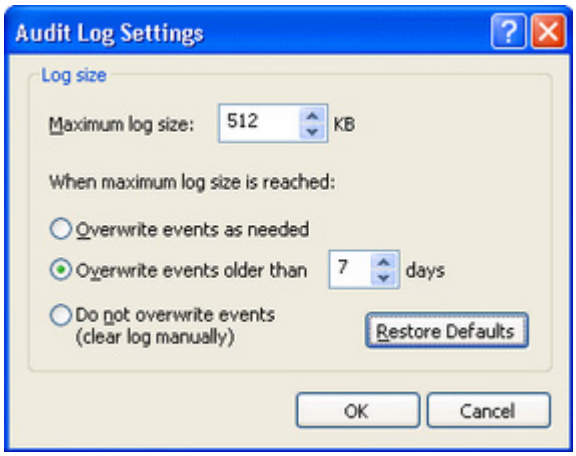
- **Type**: la classe d'un événement, à savoir **Success** lorsque l'accès a été autorisé et **Failure** lorsque l'accès a été refusé.
- **Date/Time**: la date et l'heure auxquelles un événement s'est produit.
- **Source**: le type de périphérique ou de protocole impliqué.
- **Action**: le type d'activité de l'utilisateur.
- **Name**: le nom de l'objet (fichier, clé USB, etc.).
- **Informations**: les autres informations propres au périphérique en rapport avec l'événement, comme les codes d'accès, les noms de périphériques, etc.
- **User**: le nom de l'utilisateur associé à cet événement.
- **PID**: l'identifiant de la procédure associée à cet événement.
- **Process**: le chemin d'accès du fichier d'exécution de la procédure. Dans certains cas, le nom de la procédure peut-être affiché en lieu et place du chemin d'accès.

Pour mettre à jour la liste des événements, sélectionnez l'élément **Refresh** du menu contextuel disponible en cliquant droit ou utilisez le bouton approprié sur la barre d'outils.

Pour supprimer tous les événements du journal d'audit, sélectionnez **Clear** dans le menu contextuel ou utilisez le bouton approprié sur la barre d'outils.

Audit Log Settings (Service)

Pour définir une taille maximale du journal d'événement et spécifier ce que Windows doit faire si ce fichier est plein, allez dans **Settings** à l'aide du menu contextuel du visionneur ou utilisez le bouton approprié sur la barre d'outils.



Le paramètre **Maximum log size** permet de définir la taille maximale du fichier journal (en kilo-octets). Le fichier journal est créé et utilisé uniquement par le service du journal événementiel de Windows. Ce fichier est normalement placé dans le répertoire ***%SystemRoot%\system32\config*** et intitulé ***DeviceLo.evt***.

Pour spécifier ce que doit faire Windows lorsque le registre d'événements est plein (lorsque la taille maximale définie dans **Maximum log size** est atteinte), choisissez parmi les options suivantes:

- **Overwrite events as needed**: le système écrasera les anciens événements si la taille maximale est atteinte.
- **Overwrite events older than**: les enregistrements moins anciens que cette valeur (spécifiée en jours) ne seront pas écrasés.
- **Do not overwrite events (clear log manually)**: le système n'écrasera pas les anciens événements si la taille maximale est atteinte, et il vous faudra supprimer des événements manuellement.

Remarque: Lorsque le registre est plein et que Windows ne peut écraser aucun enregistrement, DeviceLock Service ne peut plus écrire de nouveaux enregistrements dans ce registre.

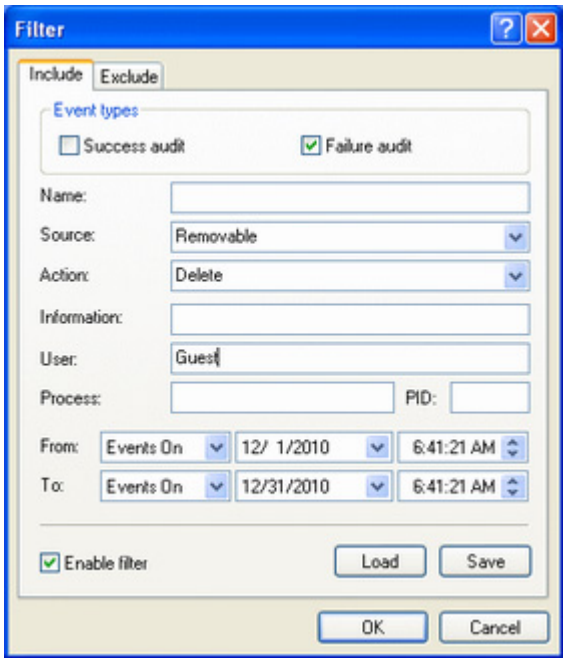
Si vous voulez retrouver les valeurs par défaut, utilisez le bouton **Restore Defaults**. Voici les valeurs par défaut:

- Le paramètre **Maximum log size** a pour valeur 512 kilo-octets.
- L'option **Overwrite events older than** est sélectionnée et fixée à 7 jours.

Audit Log Filter (Service)

Les données de l'Audit Log Viewer peuvent être filtrées afin de n'afficher que les enregistrements qui répondent aux critères indiqués.

Pour ouvrir la boîte de dialogue **Filter**, allez dans **Filter** à l'aide du menu contextuel du visionneur ou utilisez le bouton approprié sur la barre d'outils.



Deux types de filtre sont disponibles:

- **Include**: seuls les enregistrements qui répondent aux conditions spécifiées sur l'onglet **Include** apparaissent dans la liste.
- **Exclude**: les enregistrements qui répondent aux conditions spécifiées sur l'onglet **Exclude** n'apparaissent pas dans la liste.

Pour utiliser un filtre, il faut d'abord l'activer. Cochez la case **Enable filter** pour l'activer. Pour désactiver un filter de façon temporaire, décochez la case **Enable filter**.

Lorsque le filtre est actif, vous pouvez le définir en saisissant des valeurs dans les champs suivants:

- **Success audit**: indique s'il faut ou non filtrer les tentatives d'accès au périphérique réussies.
- **Failure audit**: indique s'il faut ou non filtrer les tentatives d'accès au périphérique qui ont échoué.
- **Name**: le texte qui correspond à une valeur de la colonne **Name** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).

- **Source**: le texte qui correspond à une valeur de la colonne **Source** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Action**: le texte qui correspond à une valeur de la colonne **Action** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Information**: le texte qui correspond à une valeur de la colonne **Information** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **User**: le texte qui correspond à une valeur de la colonne **User** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Process**: le texte qui correspond à une valeur de la colonne **Process** du visionneur de journal d'audit. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **PID**: le numéro qui correspond à une valeur de la colonne **PID** du visionneur de journal d'audit.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **From**: indique le début de la période qui contient les éléments que vous voulez voir. Sélectionnez **First Event** pour voir les événements en commençant par le premier enregistrement du journal. Sélectionnez **Events On** pour voir les événements ayant eu lieu à partir d'une date et une heure données.
- **To**: indique la fin de la période qui contient les éléments que vous voulez voir. Sélectionnez **Last Event** pour voir les événements en terminant par le dernier enregistrement du journal. Sélectionnez **Events On** pour voir les événements ayant eu lieu jusqu'à une date et une heure données.

L'opérateur logique AND s'applique à tous les champs spécifiés et entre les filtres actifs (Include/Exclude). Autrement dit, le résultat du filtre n'inclut que les enregistrements qui répondent à tous les critères donnés.

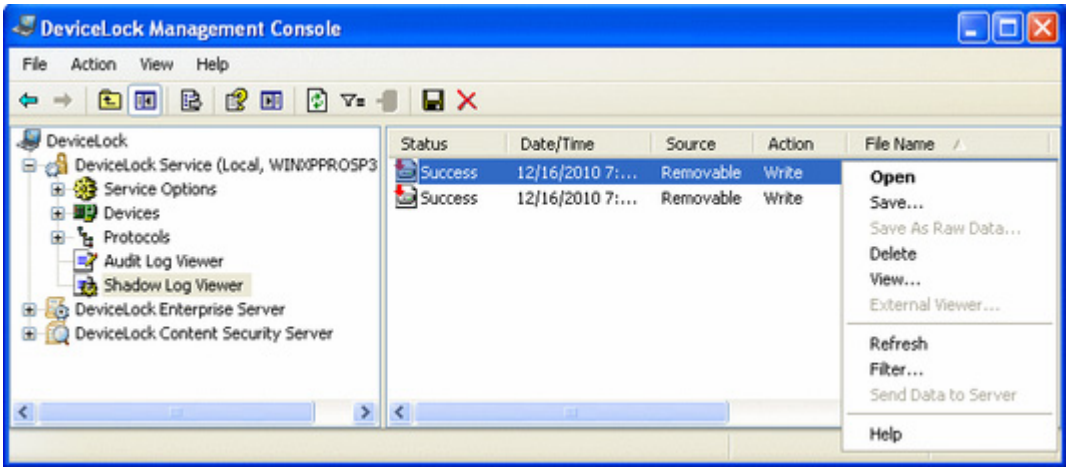
Si vous ne voulez pas qu'un champ figure dans la condition du filtre, laissez-le vierge.

Pour certains champs, l'utilisation de jokers est acceptée. Un joker est un caractère de type astérisque (*) ou point d'interrogation (?), utilisé pour remplacer un ou plusieurs caractères pour la définition d'un filtre. L'astérisque remplace zéro ou plusieurs caractères. Si vous recherchez un nom qui commence par «win» mais dont la fin vous échappe, tapez: **win***. Vous récupérerez tous les noms qui commencent par «win»", y compris Windows, Winner et

Wind. Le point d'interrogation remplace un caractère et un seul du nom. Par exemple, si vous tapez **win?**, vous obtiendrez Wind mais ni Windows ni Winner.

Shadow Log Viewer (Service)

Il s'agit d'un visionneur de journal de réplication qui permet de récupérer le journal de réplication de DeviceLock Service.



La configuration par défaut suppose que les données de réplication sont stockées sur DeviceLock Enterprise Server. Dans ce cas, toutes les données de réplication préalablement enregistrées et stockées temporairement par DeviceLock Service sur l'ordinateur local sont périodiquement transférées sur le serveur. Le journal de réplication local est vidé dès que les données ont été transférées vers le serveur; pour visionner ces données, vous devez donc utiliser le Shadow Log Viewer du serveur.

Néanmoins, dans certains cas de figure, vous aurez peut-être besoin de visionner le journal de réplication d'un ordinateur particulier. Ce besoin peut survenir par exemple si vous n'utilisez pas du tout DeviceLock Enterprise Server ou si vous utilisez le serveur mais que, pour une raison ou une autre, les données sont encore sur l'ordinateur client.

Les colonnes de ce visionneur sont les suivantes:

- **Status**: indique le statut de l'élément. Le statut **Success** (succès) indique que la donnée est bien enregistrée; le statut **Incomplete** (incomplet) indique que la donnée n'est probablement pas complètement enregistrée, alors que le statut **Failed** (échec) est attribué aux réplications de fichiers dont la transmission a été bloquée par les règles contextuelles.
- **Date/Time**: la date et l'heure du transfert de données.
- **Source**: le type de périphérique ou de protocole impliqué.
- **Action**: le type d'activité de l'utilisateur.
- **File Name**: le chemin d'accès initial vers le fichier, ou le nom généré automatiquement si les données n'étaient pas à l'origine un fichier (par exemple des

images de CD/DVD, des données écrites directement sur le média ou transférées par les ports parallèle/série).

- **File Size**: la taille des données.
- **User**: le nom de l'utilisateur qui a transféré les données.
- **PID**: l'identifiant du processus utilisé pour le transfert de données.
- **Process**: le chemin d'accès du fichier d'exécution de la procédure. Dans certains cas, le nom de la procédure peut-être affiché en lieu et place du chemin d'accès.

Utilisez le menu contextuel accessible par simple clic droit de votre souris sur chaque enregistrement.

Open (Ouvrir)
Pour ouvrir le fichier à partir d'un enregistrement sèlectionnè avec l'application associèe, cliquez sur **Open** dans le menu contextuel. Si aucune application n'est associèe, la boîte de dialogue "**Open With**" s'affiche. Si aucune donnèe n'est associèe à l'enregistrement (taille nulle ou aucun enregistrement), **Open** est dèsactivè.

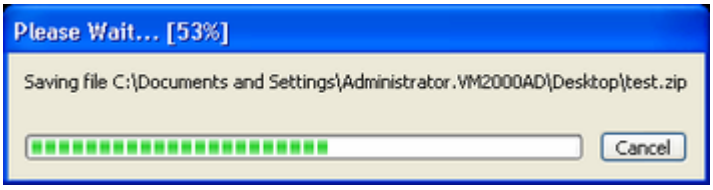
Si vous utilisez **Open** pour répliquer des données capturées à partir de périphériques de types soit Printer, soit Parallel port, l'applications associée est toujours la visionneuse intégrée dénommée DeviceLock Printer Viewer.

DeviceLock Printer Viewer permet d'afficher le document imprimé répliqué au format natif du spooler d'imprimante, de le renvoyer à l'imprimante, ou de l'enregistrer sous forme de fichier graphique (de type BMP, GIF, JPEG, PNG, EMF ou TIFF). Les formats de spooler d'imprimante suivants sont pris en charge: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, impression GDI (ZjStream) et fichiers spoolés EMF.

Save (Enregistrer)
Si vous devez sauvegarder les données d'un enregistrement sélectionné sur votre ordinateur local, utilisez l'option **Save** du menu contextuel ou cliquez sur l'icône correspondante dans la barre d'outils. Les touches Ctrl et/ou Maj permettent de sélectionner et d'enregistrer les données de plusieurs enregistrements en même temps.

Si l'enregistrement n'a pas de données associées (elles sont de taille 0 ou n'ont pas été enregistrées), l'option **Save** est désactivée dans le menu contextuel et sur la barre d'outils.

La barre de progression apparaît lorsque vous enregistrez un fichier de grande taille.



Vous pouvez appuyer à tout moment sur **Cancel** pour annuler le processus d'enregistrement. Dans ce cas, le fichier restant sur l'ordinateur local ne sera pas complet et ne contiendra que les données reçues avant l'annulation du processus d'enregistrement.

Si l'utilisateur a transféré les données sous forme de fichier, elles sont stockées dans le journal de réplication en tant que fichier et pourront être enregistrées sur l'ordinateur local sous cette forme.

Lorsque c'est vers un CD/DVD que l'utilisateur a transféré des données, celles-ci sont stockées dans le journal de réplication sous forme d'image CD/DVD unique (une image par CD/DVD inscrit ou par session), au format CUE.

Les images CD/DVD, ainsi que les autres données qui n'ont pas été transférées sous forme de fichier (accès direct au média ou transfert par port parallèle ou série) reçoivent des noms générés automatiquement d'après le type d'action, la lettre du lecteur ou le nom du périphérique, ainsi que l'heure et la date (par exemple, direct_write(E:) 19:18:29 17.07.2006.bin).

Les images CD/DVD sont enregistrées sur l'ordinateur local dans deux fichiers : le fichier de données, dont l'extension est .bin (par ex., direct_write(E_) 19_18_29 17_07_2006.bin) et

le fichier d'informations (cue sheet) qui a le même nom que le fichier de données associé, avec l'extension .cue (par exemple, direct_write(E_) 19_18_29 17_07_2006_bin.cue). Les deux fichiers sont nécessaires pour ouvrir l'image CD/DVD dans un logiciel externe qui accepte le format CUE (tel que Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO et d'autres encore).

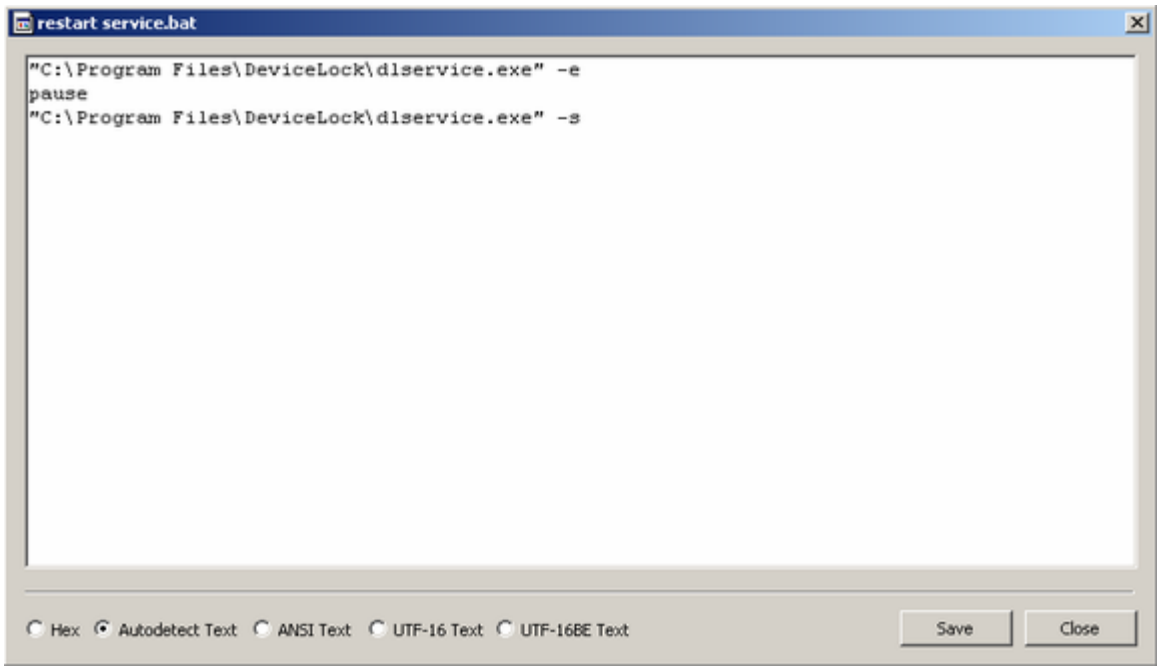
Save As Raw Data (Enregistrer en tant que données brutes)
Lorsque vous sélectionnez un enregistrement qui contient des données écrites à l'origine sous forme de session supplémentaire sur un disque CD/DVD multisession, l'élément **Save As Raw Data** est disponible dans le menu contextuel. Cet élément permet l'enregistrement tel quel sur l'ordinateur local (sans faire référence aux données des sessions précédentes).

Si vous utilisez la fonction habituelle d'enregistrement, (l'élément **Save** du menu ou l'icône de la barre d'outils), DeviceLock Management Console détecte que l'image de CD/DVD contient une session qui se rapporte à d'autres sessions (précédentes). Puisque les sessions précédentes ne sont pas disponibles (elles peuvent avoir été écrites à partir d'un ordinateur sur lequel DeviceLock Service n'est pas installé), DeviceLock Management Console retrouve et répare toutes les références à ces sessions inexistantes: ce qui fait que le fichier .cue peut être lu par les logiciels qui acceptent ce format.

Néanmoins, si vous avez besoin de données que DeviceLock Management Console n'a pas modifiées, utilisez **Save As Raw Data**. Dans ce cas, le fichier enregistré risque de ne pas être exploitable par les logiciels qui acceptent le format CUE.

Lors de l'enregistrement de fichiers de grande taille, vous pouvez appuyer sur l'option **Cancel** de la barre de progression pour annuler le processus d'enregistrement. Dans ce cas, le fichier restant sur l'ordinateur local ne contiendra que les données reçues avant l'annulation du processus d'enregistrement.

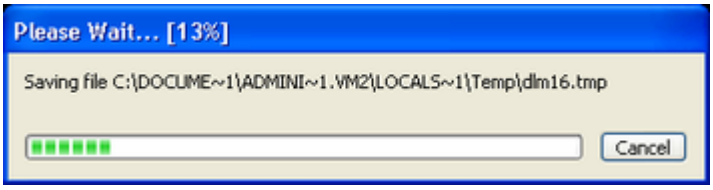
View (Visionner)
Pour ouvrir les données avec la visionneuse intégrée, utilisez **View** à l'aide du menu contextuel.



Dans le module d'affichage intégré, cliquez sur l'une ou l'autre des options d'affichage suivantes:

- **Hex** affiche les données sous forme hexadécimale et aussi de mots.
- **Autodetect Text** Permet la détection automatique du codage de texte et affiche les données au format texte uniquement.
- **ANSI Text** Indique le codage ANSI du texte et affiche les données au format texte uniquement.
- **UTF-16 Text** Indique le codage UTF-16 du texte et affiche les données au format texte uniquement.
- **UTF-16BE Text** Indique le codage Unicode UTF-16 (Big Endian) du texte et affiche les données au format texte uniquement.

Lors de l'ouverture d'un fichier de grande taille, vous pouvez appuyer sur l'option **Cancel** de la barre de progression pour annuler le processus d'ouverture.



Dans ce cas, la visionneuse n'affichera que les données reçues avant l'annulation du processus d'ouverture.

Cliquez sur **Save** pour enregistrer les données de la visionneuse dans un fichier externe.

External Viewer (Visionneur externe)
Vous pouvez aussi définir le logiciel externe à utiliser pour examiner les données répliquées. Si une visionneuse externe a été définie, l'élément **External Viewer** du menu contextuel est activé. Pour le définir, ouvrez **Regedit** et configurez l'entrée suivante sur l'ordinateur qui exécute DeviceLock Management Console :

- Clé: **HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager**
- Nom: **ExternalShadowViewer**
- Type: **REG_SZ**
- Valeur: <*chemin_compet_au_visionneur*> **%1**
  où <*chemin_compet_au_visionneur*> est à remplacer par le chemin d'accès complet vers le logiciel externe. Si ce chemin contient des espaces, utilisez des guillemets. Par exemple: "C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1.

Lors de l'ouverture d'un fichier de grande taille, vous pouvez appuyer sur l'option **Cancel** de la barre de progression pour annuler le processus d'ouverture. Dans ce cas, le logiciel externe n'affichera que les données reçues avant l'annulation du processus d'ouverture.

Delete (Supprimer)
Pour supprimer un enregistrement, choisissez l'option **Delete** du menu contextuel ou utilisez le bouton approprié sur la barre d'outils. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

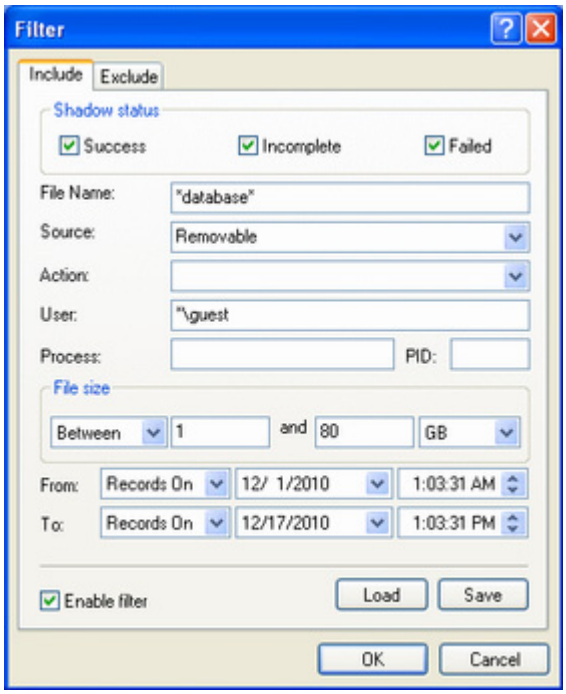
Refresh (Mettre à jour)
Pour mettre à jour la liste, sélectionnez l'élément **Refresh** du menu contextuel disponible en cliquant droit ou utilisez le bouton approprié sur la barre d'outils.

Send Data to Server (Envoyer les données au serveur)
Lorsque DeviceLock Enterprise Server est défini dans les Service Options et que vous devez forcer le transfert des données répliquées de l'ordinateur local au serveur, utilisez l'option **Send Data to Server** du menu contextuel, disponible en cliquant droit ou utilisez le bouton approprié sur la barre d'outils.

Shadow Log Filter (Service)

Les données du Shadow Log Viewer peuvent être filtrées afin de ne voir que les enregistrements qui répondent aux critères indiqués.

Pour ouvrir la boîte de dialogue **Filter**, allez dans **Filter** à l'aide du menu contextuel du visionneur, ou utilisez le bouton approprié sur la barre d'outils.



Il n'y a que peu de différences entre la définition des filtres du journal d'audit et celle des filtres du journal de réplication: consultez donc tout d'abord le chapitre Audit Log Filter (Service) de ce manuel.

Lorsque le filtre est actif, vous pouvez le définir en saisissant des valeurs dans les champs suivants:

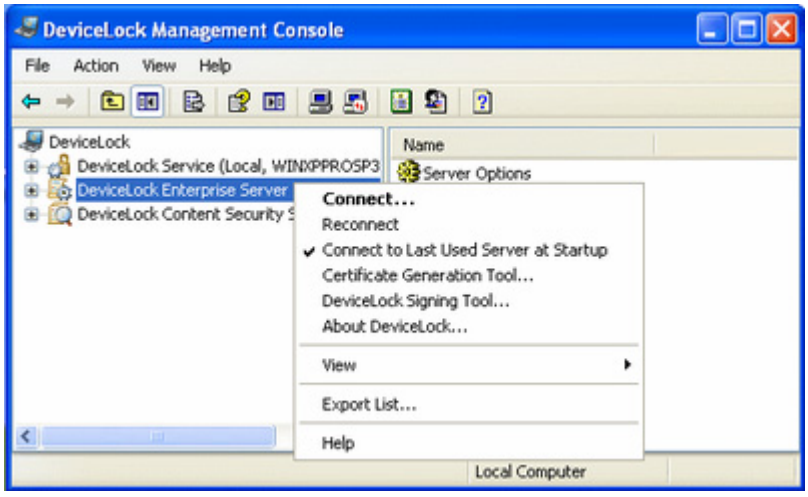
- **Success**: spécifie s'il faut ou non filtrer les données enregistrées avec succès.
- **Incomplete**: spécifie s'il faut ou non filtrer les données enregistrées de façon partielle.
- **Failed**: indique s'il faut filtrer ou non les données de journal dont la transmission a été bloquée par des règles contextuelles.
- **File Name**: le texte qui correspond à une valeur de la colonne **File Name** du visionneur de journal de réplication. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Source**: le texte qui correspond à une valeur de la colonne **Source** du visionneur de journal de réplication.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Action**: le texte qui correspond à une valeur de la colonne **Action** du visionneur de journal de réplication.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **User**: le texte qui correspond à une valeur de la colonne **User** du visionneur de journal de réplication. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.

Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).

- **Process**: le texte qui correspond à une valeur de la colonne **Process** du visionneur de journal de réplication. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **PID**: le numéro qui correspond à une valeur de la colonne **PID** du visionneur de journal de réplication.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **File size**: le nombre ou la plage de nombres qui correspond à une valeur de la colonne **File Size** du visionneur de journal de réplication.
- **From**: indique le début de la période qui contient les enregistrements que vous voulez voir. Sélectionnez **First Event** pour voir les enregistrements en commençant par le premier enregistrement du journal. Sélectionnez **Records On** pour voir les enregistrements qui ont été écrits à partir d'une date et d'une heure données.
- **To**: indique la fin de la période qui contient les enregistrements que vous voulez voir. Sélectionnez **Last Record** pour voir les enregistrements, en terminant par le dernier enregistrement du journal. Sélectionnez **Records On** pour voir les enregistrements qui ont été écrits jusqu'à une date et une heure données.

Administration de DeviceLock Enterprise Server

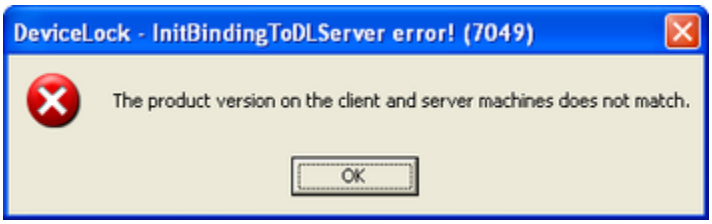
Développez l'élément **DeviceLock Enterprise Server** pour accéder à toutes les fonctionnalités et tous les paramètres de configuration d'un serveur.



Un menu contextuel est disponible: cliquez droit sur l'élément **DeviceLock Enterprise Server** en question:

- **Connect**: se connecte à tout ordinateur spécifié. Pour plus d'informations, veuillez lire le chapitre Connexion aux ordinateurs de ce manuel.

Lors d'une connexion à un ordinateur équipé d'une ancienne version de DeviceLock Enterprise Server, le message suivant peut apparaître.

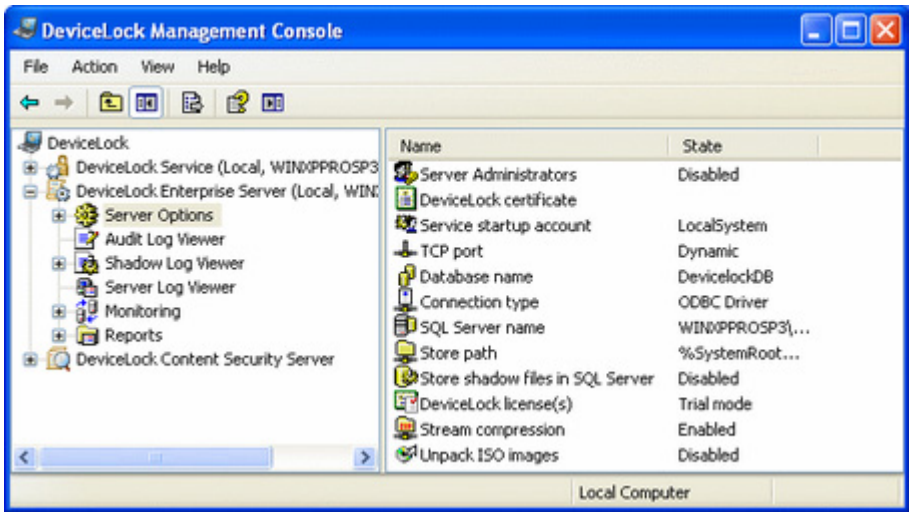


Dans ce cas, vous devez installer la nouvelle version de DeviceLock Enterprise Server sur cet ordinateur. Pour des renseignements sur l'installation de DeviceLock Enterprise Server, veuillez vous reporter à la section Installation de DeviceLock Enterprise Server de ce manuel.

- **Reconnect**: renouvelle la connexion à l'ordinateur actuellement connecté.
- **Connect to Last Used Server at Startup**: cochez cette option pour ordonner à DeviceLock Management Console de se connecter automatiquement au serveur utilisé en dernier lieu à chaque démarrage.
- **Certificate Generation Tool**: lance l'outil spécial qui permet de générer des DeviceLock Certificates. Pour plus d'information, veuillez lire le chapitre Création de DeviceLock Certificates de ce manuel.
- **DeviceLock Signing Tool**: exécute l'outil spécial qui permet d'accorder aux utilisateurs un accès temporaire aux périphériques demandés et de signer les fichiers XML avec les paramètres de DeviceLock Service. Pour plus d'informations, reportez-vous à la section DeviceLock Signing Tool de ce manuel.
- **About DeviceLock**: ouvre une boîte de dialogue contenant des informations sur la version de DeviceLock employée et sur vos licences.

Server Options (Options de serveur)

Ces paramètres supplémentaires permettent d'améliorer encore la configuration de DeviceLock Enterprise Server.



Utilisez le menu contextuel affiché en cliquant droit sur la souris, ou double-cliquez sur le paramètre **Stream compression** pour l'activer ou le désactiver. En activant le paramètre **Stream compression**, vous ordonnez à DeviceLock de compresser les journaux d'audit et les données de réplication de DeviceLock Services pour les envoyer vers DeviceLock Enterprise Server. La taille des transferts de données est ainsi réduite, ce qui permet d'alléger la charge du réseau.

Le fait d'activer le paramètre **Unpack ISO images** permet de demander à DeviceLock Enterprise Server d'extraire les fichiers des images CD/DVD répliquées. Si ce paramètre est activé, tous les fichiers sont extraits des images CD/DVD lors de leur livraison au serveur et stockées dans la base de données de façon séparée (une donnée par fichier). Sinon, les images CD/DVD répliquées entières sont stockées dans la base de données.

Utilisez le menu contextuel avec d'autres paramètres pour ouvrir les boîtes de dialogue qui permettent de procéder à des modifications. Vous pouvez aussi double-cliquer sur le paramètre pour ouvrir la boîte de dialogue.

Le chapitre Installation de DeviceLock Enterprise Server du présent manuel décrit en détail tous ces paramètres.

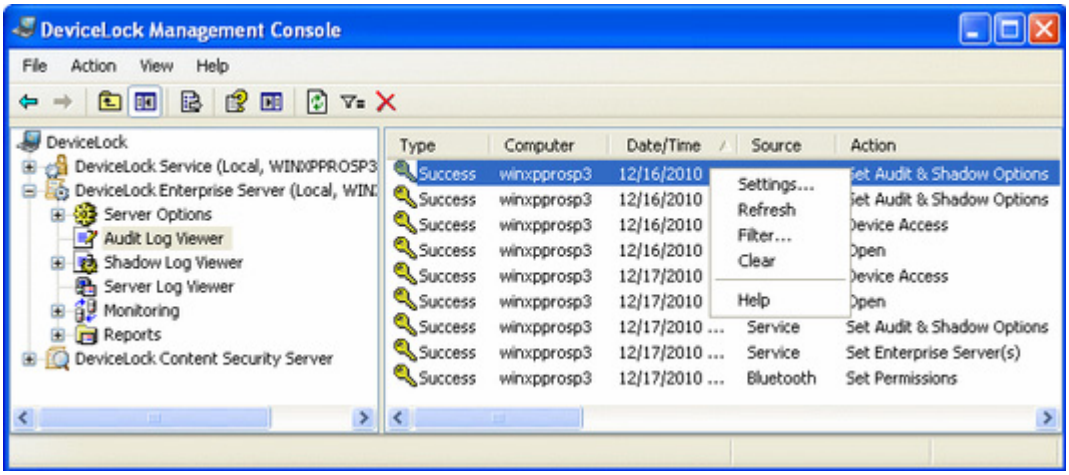
Pour lancer l'assistant de configuration et vérifier ou renseigner point par point tous les paramètres, utilisez l'élément **Properties** du menu contextuel de **Server Options**. L'assistant de configuration est aussi décrit dans le chapitre Installation de DeviceLock Enterprise Server du présent manuel.

Audit Log Viewer (Server)

Le visionneur de journal d'audit permet la récupération du journal d'audit stocké sur DeviceLock Enterprise Server.

DeviceLock Enterprise Server ne stocke les donnés d'audit reçues d'un ordinateur distant que si l'option **DeviceLock Log** ou **Event & DeviceLock Logs** est sélectionnée dans le

paramètre **Audit log type** des Service Options de l'ordinateur considéré. Sinon, les données d'audit sont stockées dans le sous-système local de journalisation des événements Windows de l'ordinateur distant et peuvent être visualisés à l'aide du visionneur de journal d'audit du service.



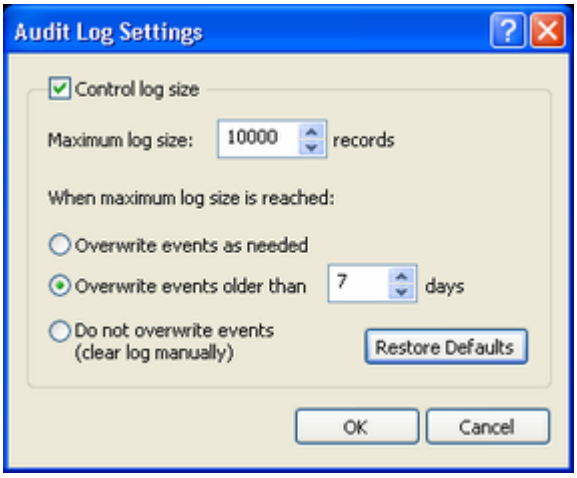
Il y a peu de différences entre le visionneur de journal d'audit du service et celui du serveur. Nous vous invitons donc à lire la section Audit Log Viewer (Service) de ce manuel.

Par rapport au module de visualisation du journal d'audit du service, celui du serveur a les colonnes supplémentaires suivantes:

- **Computer**: le nom de l'ordinateur dont proviennent les journaux d'audit.
- **Event**: un numéro qui identifie le type d'événement considéré.
- **Received Date/Time**: indique la date et l'heure de réception de l'événement par DeviceLock Enterprise Server.

Audit Log Settings (Server)

Pour définir une taille maximale de journal et spécifier ce que DeviceLock Enterprise Server doit faire si le journal d'audit est plein, utilisez les **Settings** du menu contextuel de l'Audit Log Viewer.



Remarque: Ces paramètres sont stockés dans la base de données et dépendent du journal, et non du DeviceLock Enterprise Server considéré. Autrement dit, si plusieurs DeviceLock Enterprise Servers utilisent une même base de données, tous possèdent les mêmes paramètres de journal.

Cochez la case **Control log size** pour permettre à DeviceLock Enterprise Server de contrôler le nombre de données dans le journal et pour supprimer les données périmées (le cas échéant) afin de libérer de l'espace pour les nouvelles données. Sinon, si la case **Control log size** est décochée, DeviceLock Enterprise Server utilise tout l'espace disponible de la base de données du SQL Server pour stocker le journal.

Le paramètre **Maximum log size** permet de spécifier le nombre maximum de données que ce journal peut contenir. Remarque: si cette base de données est utilisée par plus d'un DeviceLock Enterprise Server, le nombre réel de données dans le journal peut être un peu plus élevé (de quelques unités) que la valeur en question.

Pour spécifier ce que doit faire DeviceLock Enterprise Server lorsque le journal est plein (lorsque la taille maximale définie dans **Maximum log size** est atteinte), choisissez une des options suivantes :

- **Overwrite events as needed**: le système écrasera les anciens événements si la taille maximale est atteinte.
- **Overwrite events older than**: les enregistrements moins anciens que cette valeur (spécifiée en jours) ne seront pas écrasés.
- **Do not overwrite events (clear log manually)**: le serveur n'écrasera pas les anciens événements si la taille maximale est atteinte, et il vous faudra supprimer des événements manuellement.

Pour retrouver les valeurs par défaut, utilisez le bouton **Restore Defaults**. Voici les valeurs par défaut:

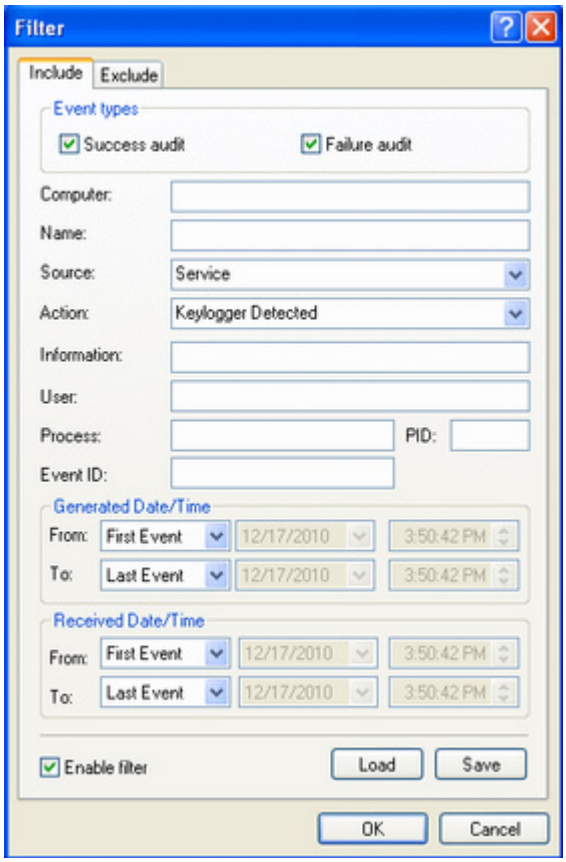
- La valeur du paramètre **Maximum log size** est fixée a 10000 données.
- L'option **Overwrite events older than** est sélectionnée et fixée a 7 jours.

S'il n'y a pas de place pour les nouvelles données dans le journal d'audit et qu'il n'y a rien à supprimer, DeviceLock Enterprise Server ne supprime pas les données d'audit des ordinateurs distants de l'utilisateur. Cela évite de perdre les données d'audit à cause d'un manque de place dans le journal. Lorsque de l'espace se libère dans le journal, DeviceLock Enterprise Server transfère les données d'audit restantes des ordinateurs des utilisateurs vers le journal en question.

Audit Log Filter (Server)

Les données de l'Audit Log Viewer peuvent être filtrées afin de n'afficher que les enregistrements qui répondent aux critères indiqués dans la liste.

Pour ouvrir la boîte de dialogue **Filter**, utilisez l'option **Filter** du menu contextuel du visionneur de journal d'audit, ou appuyez sur le bouton approprié dans la barre d'outils.



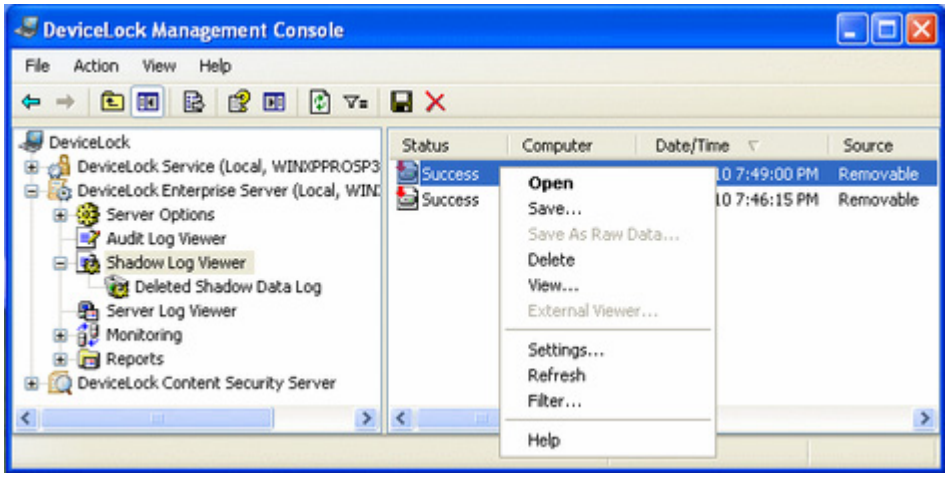
Il y a peu de différences entre le filtre de journal d'audit du service et celui du serveur. Nous vous invitons donc à lire la section Audit Log Filter (Service) de ce manuel.

Par rapport au filtre du journal d'audit du service, celui du serveur n'a que les champs supplémentaires suivants:

- **Computer**: ce texte correspond a une valeur de la colonne **Computer** du visionneur de journal d'audit. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Event ID**: ce numéro correspond à une valeur de la colonne **Event** du visionneur de journal d'audit.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Received Date/Time**: précise l'intervalle de temps pour le filtrage des événements en fonction du moment auquel DeviceLock Enterprise Server les reçoit. **From:** indique la date et l'heure des premiers événements que vous désirez filtrer, tandis que **To:** indique la date et l'heure des derniers événements. Les différentes valeurs possibles du paramètre **From:** sont: **First Event**, **Events On**. Sélectionnez **First Event** pour voir les évènements en commençant par le premier événement reçu par DeviceLock Enterprise Server. Sélectionnez **Events On** pour voir les évènements reçus en commençant par une date et une heure précises. Les différentes valeurs possibles du paramètre **To:** sont: **Last Event**, **Events On**. Sélectionnez **Last Event** pour voir les évènements en terminant par le dernier événement reçu par DeviceLock Enterprise Server. Sélectionnez **Events On** pour voir les évènements reçus en terminant par une date et une heure précises.

Shadow Log Viewer (Server)

Le visionneur de journal de réplication permet la récupération du journal de réplication stocké sur DeviceLock Enterprise Server.



Il y a peu de différences entre le visionneur de journal de réplication du service et celui du serveur. Nous vous invitons donc à lire la section Shadow Log Viewer (Service) de ce manuel.

Par rapport au module de visualisation du journal de réplication du service, celui du serveur n'a que deux colonnes supplémentaires:

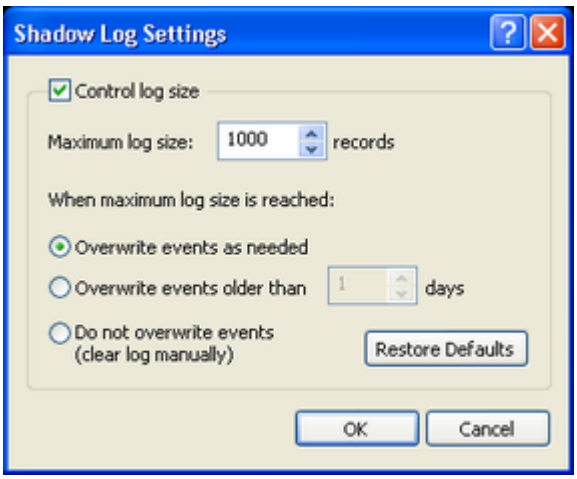
- **Computer**: le nom de l'ordinateur dont provient le journal de réplication.
- **Received Date/Time**: indique la date et l'heure de réception de l'événement par DeviceLock Enterprise Server.

A l'inverse du visionneur de journal de réplication du service, lorsque vous supprimez un enregistrement dans le visionneur du serveur, les données binaires sont éliminées de la base de données ou du disque (selon l'état du paramètre Store shadow files in SQL Server) mais toutes les autres informations (nom et taille du fichier, nom d'utilisateur, date et heure, processus et ainsi de suite) sont déplacées vers un journal spécial appelé Deleted Shadow Data Log.

Ce journal des données répliquées et effacées sert lorsque vous n'avez plus besoin du contenu des données répliquées et que vous voulez libérer de l'espace de stockage (dans le serveur SQL ou sur le disque), mais que vous devez encore garder des informations sur le transfert de données.

Shadow Log Settings (Paramètres du journal de réplication)

Pour définir une taille maximale de journal et spécifier ce que DeviceLock Enterprise Server doit faire si le journal de réplication est plein, utilisez l'option **Settings** du menu contextuel du Visionneur de journal de réplication.



Pour plus d'informations sur ces paramètres, veuillez vous reporter à la section Audit Log Settings (Server) de ce manuel.

Lorsque DeviceLock Enterprise Server doit supprimer certaines données anciennes du journal de replication à cause de paramètres définis (**Overwrite events as needed** et **Overwrite events older than**), ces données sont transférées dans le Deleted Shadow Data Log (journal des données de réplication supprimées).

S'il n'y a pas de place pour les nouvelles données dans le journal de réplication et qu'il n'y a rien à supprimer, DeviceLock Enterprise Server ne supprime pas les données de réplication des ordinateurs distants de l'utilisateur. Cela évite de perdre les données de réplication à

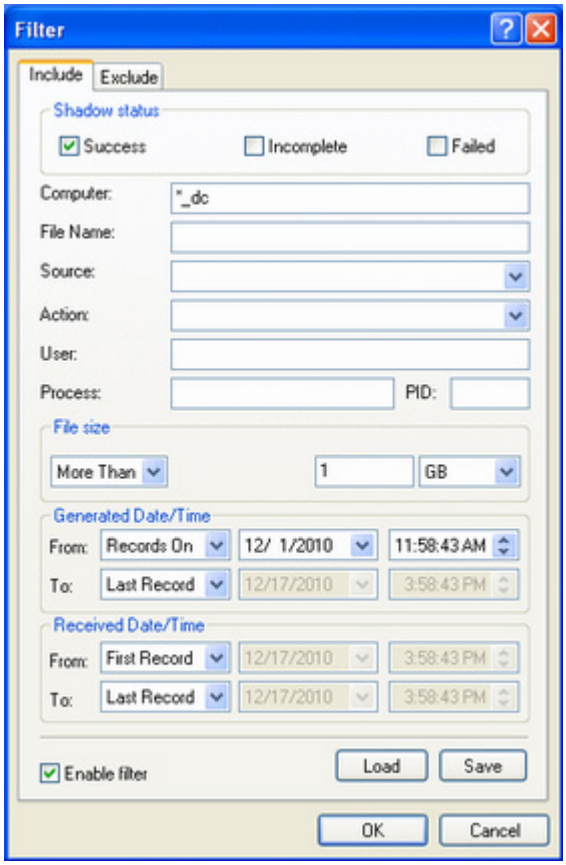
cause d'un manque de place dans le journal. Lorsque de l'espace se libère dans le journal, DeviceLock Enterprise Server transfère les données de réplication restantes des ordinateurs des utilisateurs vers le journal en question.

Il vaut mieux éviter d'accumuler des données de réplication sur les ordinateurs des utilisateurs. Nous conseillons de surveiller le journal du DeviceLock Enterprise Server à intervalles réguliers, d'être attentif aux avertissements qu'il contient et d'adapter les paramètres de journal en conséquence.

Shadow Log Filter (Server)

Les données du Shadow Log Viewer peuvent être filtrées afin de ne voir que les enregistrements qui répondent aux critères indiqués.

Pour ouvrir la boîte de dialogue **Filter**, allez dans **Filter** à l'aide du menu contextuel du visionneur, ou utilisez le bouton approprié sur la barre d'outils.



Il y a peu de différences entre le filtre du journal de réplication du service et celui du serveur. Nous vous invitons donc à lire la section Shadow Log Filter (Service) de ce manuel.

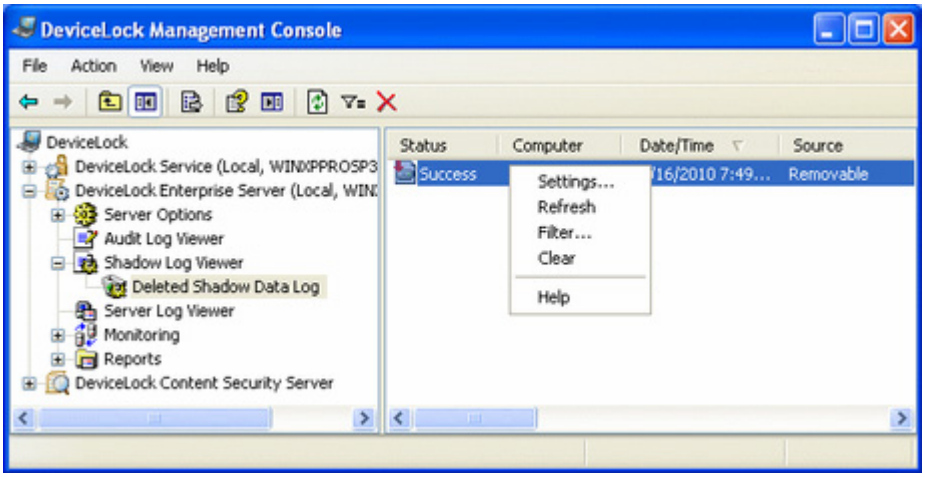
Par rapport au filtre du journal de réplication du service, celui du serveur n'a que les champs supplémentaires suivants:

- **Computer**: le texte qui correspond à une valeur de la colonne **Computer** du visionneur de journal de réplication. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Received Date/Time**: précise l'intervalle de temps de filtrage des enregistrements en fonction du moment auquel DeviceLock Enterprise Server les reçoit. **From:** indique la date et l'heure des premiers enregistrements que vous désirez filtrer, tandis que **To:** indique la date et l'heure des derniers enregistrements. Les différentes valeurs possibles du paramètre **From:** sont: **First Record**, **Records On**. Sélectionnez **First Record** pour voir les enregistrements en commençant par le premier enregistrement reçu par DeviceLock Enterprise Server. Sélectionnez **Records On** pour voir les enregistrements reçus en commençant par une date et une heure précises. Les différentes valeurs possibles du paramètre **To:** sont: **Last Record**, **Records On**. Sélectionnez **Last Record** pour voir les enregistrements reçus en terminant par le dernier enregistrement reçu par DeviceLock Enterprise Server. Sélectionnez **Records On** pour voir les enregistrements reçus en terminant par une date et une heure précises.

Deleted Shadow Data Log

Ce visionneur permet la récupération des informations des enregistrements supprimés du journal de réplication.

Lorsqu'un enregistrement est supprimé du journal du Shadow Log Viewer, les données binaires sont supprimées mais toutes les autres informations (nom et taille du fichier, nom d'utilisateur, date et heure, processus et ainsi de suite) sont transférées dans ce journal.



Ce journal sert lorsque vous n'avez plus besoin du contenu des données répliquées et que vous voulez libérer de l'espace de stockage (dans le serveur SQL ou sur le disque), mais que vous devez encore garder des informations sur le transfert de données.

Pour définir une taille de journal maximum et indiquer à DeviceLock Enterprise Server ce qu'il doit faire une fois le journal de données de réplication supprimées plein, sélectionnez l'option **Settings** du menu contextuel à l'aide du bouton droit de la souris. Ces paramètres de journal sont similaires à ceux du journal d'audit, on consultera par conséquent avec profit la section Audit Log Settings (Server) de ce manuel.

Si aucun espace n'est disponible pour de nouvelles données dans le journal des données de réplication supprimées et s'il n'y a rien à supprimer, DeviceLock Enterprise Server se contente d'ignorer les nouvelles données éventuelles. Pour éviter de perdre des données de cette façon, nous conseillons de surveiller le journal du DeviceLock Enterprise Server à intervalles réguliers et d'être attentif aux avertissements qu'il contient.

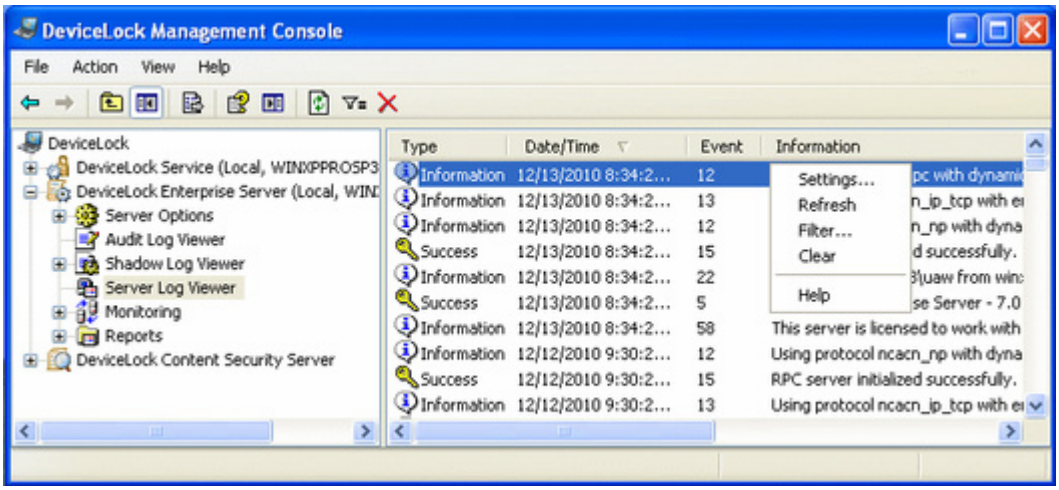
Pour mettre à jour la liste, sélectionnez l'élément **Refresh** du menu contextuel disponible en cliquant droit, ou utilisez le bouton approprié sur la barre d'outils.

Pour filtrer les enregistrements de la liste, sélectionnez l'élément **Filter** du menu contextuel disponible en cliquant droit ou utilisez le bouton approprié sur la barre d'outils. Le même filtre sert pour le visionneur de journal de réplication; veuillez consulter le chapitre Shadow Log Filter (Server) dans ce manuel pour plus d'informations.

Pour supprimer tous les événements de ce journal, sélectionnez l'option **Clear** du menu contextuel ou utilisez le bouton approprié sur la barre d'outils.

Server Log Viewer

Ce visionneur permet la récupération du journal interne de DeviceLock Enterprise Server. Le serveur enregistre les erreurs, les avertissements et d'autres informations importantes (modifications de la configuration, démarrages et arrêts, version, etc.).



Les informations de ce journal peuvent servir au diagnostique des problèmes (le cas échéant), pour suivre les modifications de la configuration du serveur et afin de savoir qui a nettoyé des journaux et quand.

Les colonnes de ce visionneur sont les suivantes:

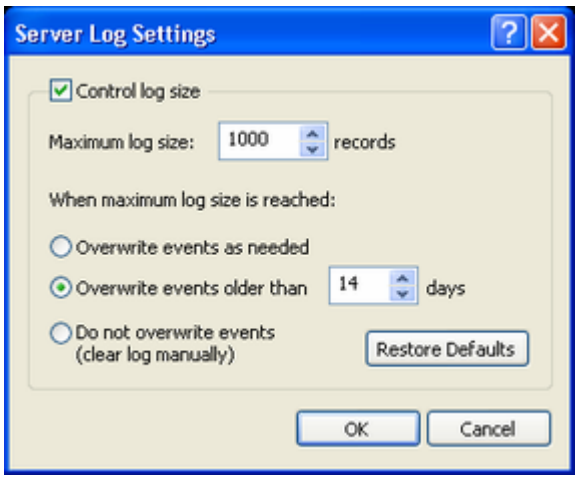
- **Type**: la classe de l'événement: **Success**, **Information**, **Warning** ou **Error**.
- **Date/Time**: la date et l'heure de l'événement.
- **Event**: un numéro qui identifie le type d'événement.
- **Information**: des informations spécifiques à l'événement: descriptions des erreurs/avertissements, noms et valeurs des paramètres modifiés, et ainsi de suite.
- **Server**: le nom du serveur sur lequel s'est produit l'événement.
- **Record N**: le numéro de l'enregistrement.

Pour mettre à jour la liste, sélectionnez l'élément **Refresh** du menu contextuel disponible en cliquant droit ou utilisez le bouton approprié sur la barre d'outils.

Pour supprimer tous les événements de ce journal, sélectionnez l'option **Clear** du menu contextuel ou utilisez le bouton approprié sur la barre d'outils. Après le nettoyage du journal du serveur, l'événement que constitue cette action de nettoyage est enregistré dans le journal (par exemple, "The Server Log (100 record(s)) was cleared by VM2000AD\Administrator from xpvirt.vm2000ad.com").

Server Log Settings

Pour définir une taille maximale de journal et spécifier ce que DeviceLock Enterprise Server doit faire si le journal de serveur est plein, utilisez l'option **Settings** du menu contextuel du Server Log Viewer.



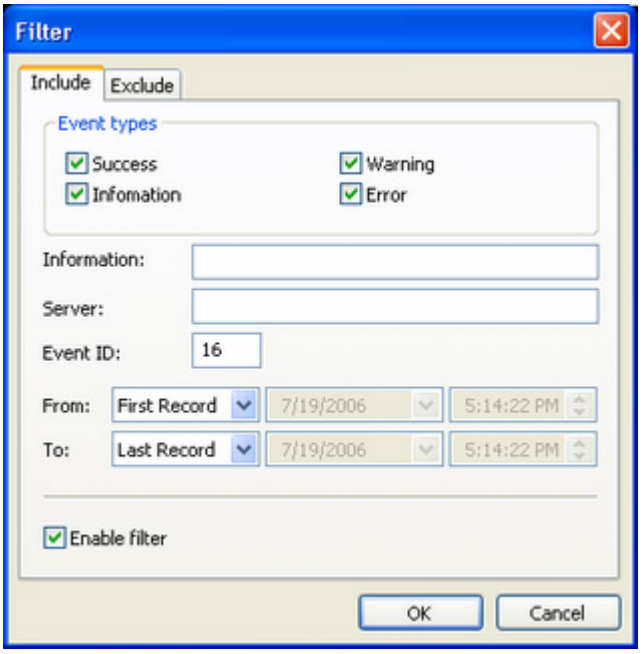
Pour plus d'informations sur ces paramètres, veuillez vous reporter à la section Audit Log Settings (Server) de ce manuel. Si aucun espace n'est disponible pour de nouvelles données dans le journal de serveur et s'il n'y a rien à supprimer, DeviceLock Enterprise Server se

contente d'ignorer les nouvelles données éventuelles.

Server Log Filter

Les données du Server Log Viewer peuvent être filtrées afin de ne voir que les enregistrements qui répondent aux critères indiqués.

Pour ouvrir la boîte de dialogue **Filter**, allez dans **Filter** à l'aide du menu contextuel du Server Log Viewer ou utilisez le bouton approprié sur la barre d'outils.



Il n'y a que peu de différences entre la définition des filtres du journal d'audit et celle des filtres du journal de serveur: consultez donc tout d'abord le chapitre Audit Log Filter (Service) de ce manuel.

Lorsque le filtre est actif, vous pouvez le définir en saisissant des valeurs dans les champs suivants:

- **Success**: spécifie s'il faut filtrer ou non les événements de la catégorie **Success**.
- **Information**: spécifie s'il faut filtrer ou non les événements de la catégorie **Information**.
- **Warning**: spécifie s'il faut filtrer ou non les événements de la catégorie **Warning**.
- **Error**: spécifie s'il faut filtrer ou non les événements de la catégorie **Error**.
- **Information**: le texte qui correspond à une valeur de la colonne **Information** du Server Log Viewer. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).

- **Server**: le texte qui correspond à une valeur de la colonne **Server** du Server Log Viewer. Ce champ n'est pas sensible a la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Event ID**: le numéro qui correspond à une valeur de la colonne **Event** du visionneur de journal de serveur.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **From**: spécifie le début de la période qui contient les éléments que vous voulez voir. Sélectionnez **First Event** pour voir les événements en commençant par le premier enregistrement du journal. Sélectionnez **Events On** pour voir les événements ayant eu lieu à partir d'une date et une heure données.
- **To**: spécifie la fin de la période qui contient les éléments que vous voulez voir. Sélectionnez **Last Event** pour voir les événements en terminant par le dernier enregistrement du journal. Sélectionnez **Events On** pour voir les événements ayant eu lieu jusqu'à une date et une heure données.

Surveillance

Cette fonctionnalitè de DeviceLock Enterprise Server permet de mettre en oeuvre une surveillance en temps rèel des DeviceLock Services dans l'ensemble du rèseau. DeviceLock Enterprise Server peut surveiller les ordinateurs distants en temps rèel, en vèrifiant le statut de DeviceLock Service (actif ou non), ainsi que la consistance et l'intègritè de la politique utilisèe. Les informations dètaillèes sont enregistrèes dans le journal spècial et peuvent être affichèes à l'aide du Monitoring Log Viewer.

Il est ègalement possible de dèfinir une politique de base susceptible d'être appliquèe à l'ensemble des ordinateurs distants sèlectionnès dans le cas où leurs politiques au moment considèrè seraient pèrimèes ou endommagèes.

De plus, vous pouvez utiliser cette fonction de recuperation de politique en tant que mèthode alternative pour dèployer des paramètres, des permissions, des règles d'audit et de réplication pour supprimer DeviceLock Services dans l'ensemble du réseau.

Présentation de l'architecture

Toutes les actions (surveillance des ordinateurs, cohèrence des politiques et vèrification d'intègritè, etc.) sont effectuèes par tâches.

Sur un DeviceLock Enterprise Server unique, vous pouvez avoir autant de tâches que vous le souhaitez. Le nombre maximum de tâches sur un serveur n'est limité que par la mémoire disponible, la capacité de la CPU et la bande passante du réseau. Veuillez tenir compte du fait que le serveur doit disposer d'assez de ressources pour communiquer avec au moins 10 ordinateurs distants en même temps.

Par défaut, DeviceLock Enterprise Server peut executer jusqu'à 30 tâches simultanément. Autrement dit, si vous avez, par exemple, 40 tâches et que toutes s'exécutent en même

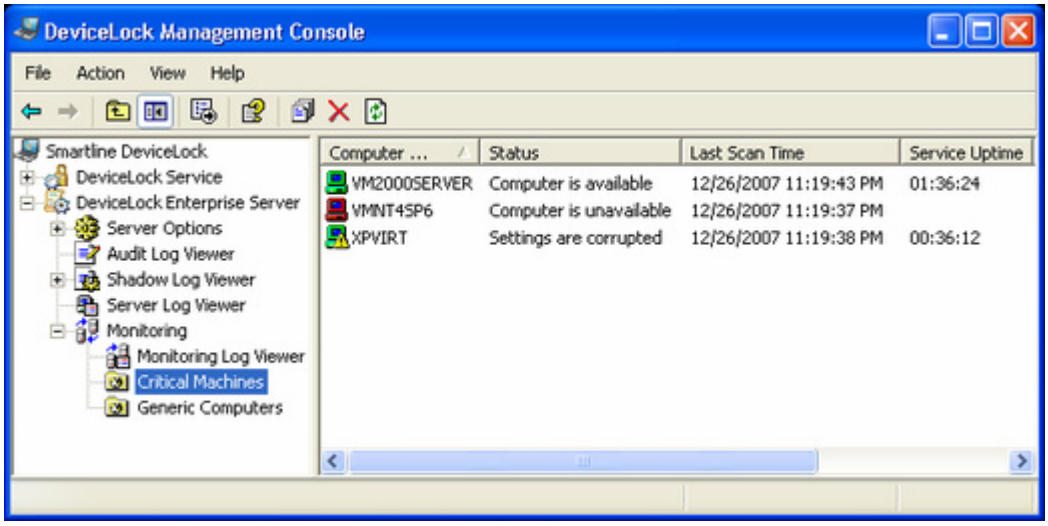
temps, les 30 premières tâches seront exécutées en premier et les 10 tâches restantes seront exécutées successivement une fois les 30 première achevées.

Cependant, vous pouvez changer le nombre de tâches susceptibles d'être exécutées simultanément en modifiant le registre. Pour définir le nouveau nombre, ouvrez **Regedit** et configurez l'entrée suivante sur l'ordinateur qui exécute DeviceLock Enterprise Server:

- Clé: **HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer**
- Nom: **ConcurrentJobs**
- Type: **DWORD**
- Valeur: *nombre_de_traitements*
  où *nombre_de_traitements* doit être une valeur comprise entre 1 et 1000.

Lors de leur exècution, les tâches enregistrent des informations de statut dans le journal de surveillance, y compris des données sur les ordinateurs et les DeviceLock Services surveillés. Elles enregistrent aussi les erreurs éventuelles qui se sont produites durant la recherche des ordinateurs et la connexion aux DeviceLock Services.

Les tâches affichent également le statut des ordinateurs surveillés et d'autres informations utiles sur la console de gestion. Vous pouvez ainsi garder un oeil sur les ordinateurs surveillés en temps réel.



Pour afficher les ordinateurs surveillès qui font partie de la tâche, mettez cette tâche en surbrillance dans l'arborescence de gauche.

Pour mettre à jour les informations affichées dans la liste des ordinateurs, sèlectionnez l'èlèment **Refresh** du menu contextuel disponible en cliquant droit ou utilisez le bouton appropriè de la barre d'outils.

- **Computer Name**: le nom de l'ordinateur surveillé.

- **Status**: le statut de l'ordinateur et du DeviceLock Service surveillé.

  Le statut affecte aussi la petite image (l'icône) affichée en regard du paramètre **Computer Name**. Les règles générales d'interprétation des icônes d'ordinateur sont les suivantes:

  - ordinateur vert: signifie que l'ordinateur fonctionne et que DeviceLock Service s'exécute dessus.
  - ordinateur rouge: signifie que l'ordinateur ne fonctionne pas ou n'a pas été trouvé, ou qu'il fonctionne mais sans DeviceLock Service.
  - ordinateur avec point d'exclamation: signifie que quelque chose ne tourne pas rond au niveau de l'ordinateur ou de DeviceLock Service.

  Il existe huit statuts différents:

  1. **Computer is available**: ce statut signifie que l'ordinateur surveillé fonctionne et que DeviceLock Service s'exécute dessus. De même, si cette tâche vérifie l'intégrité de la politique, la vérification s'est déroulée sans incident. L'icône d'ordinateur sera «ordinateur vert.»

     Si cette tâche restaure la politique interrompue, l'icône d'ordinateur sera «ordinateur vert avec point d'exclamation.»
  2. **Computer is unavailable**: ce statut signifie que DeviceLock Enterprise Server n'arrive pas à localiser l'ordinateur surveillé. Cela se produit lorsqu'un ordinateur ne fonctionne pas ou que les connexions sont bloquées par un pare-feu, mais le nom et l'adresse de l'ordinateur peuvent être trouvés via DNS. L'icône d'ordinateur sera «ordinateur rouge.»
  3. **Service is unavailable**: ce statut signifie que DeviceLock Enterprise Server n'arrive pas à se connecter à DeviceLock Service sur l'ordinateur surveillé. Cela se produit lorsque l'ordinateur fonctionne mais que DeviceLock Service ne s'exécute pas. Cela peut aussi être lié au fait d'executer DeviceLock Service sur un port TCP différent de celui indiqué dans la configuration de tâches ou à un blocage des connexions par le pare-feu. L'icône d'ordinateur sera «ordinateur rouge avec point d'exclamation.» Pour plus d'informations sur les problèmes de connexion, veuillez consulter la description du paramètre Service connection settings.
  4. **Settings are corrupted**: ce statut signifie que l'ordinateur surveillé fonctionne et que DeviceLock Service s'exécute dessus, mais que le processus de vérification de police a échoué. Cela se produit lorsque la politique principale est assignée à une tâche et qu'elle diffère de celle du DeviceLock Service surveillé. L'icône d'ordinateur sera «ordinateur vert avec point d'exclamation.»
  5. **Unresolved computer address**: ce statut signifie que DeviceLock Enterprise Server n'arrive pas à trouver le nom ou l'adresse de l'ordinateur. Cela se produit lorsqu'on spécifie un nom d'ordinateur incorrect qui n'existe pas dans le DNS. Cela peut aussi se produire en absence de serveur DNS. Dans ce cas, le statut **Unresolved computer address** doit être traité comme **Computer is unavailable**. L'icône d'ordinateur sera «ordinateur rouge avec point d'exclamation.»
  6. **Unsupported service version**: ce statut signifie que DeviceLock Enterprise Server est en train d'essayer de télécharger une politique (des paramètres de service) à partir de DeviceLock Service version 6.2 ou inférieure. La verification de politique n'est prise en charge que pour les versions 6.2.1 et

suivantes. L'icône d'ordinateur sera «ordinateur vert avec point d'exclamation.»

7. **Access is denied**: ce statut signifie que DeviceLock Enterprise Server n'arrive pas à se connecter à DeviceLock Service en raison d'un manque de privilèges. Cela se produit lorsque le compte sous lequel le service DeviceLockEnterprise Server démarre n'a aucun droit pour se connecter à DeviceLock Service. L'icône d'ordinateur sera «ordinateur vert avec point d'exclamation.» Pour plus d'informations sur la façon de résoudre ce problème, veuillez consulter la description du paramètre Service connection settings.

8. **No License**: ce statut signifie que DeviceLock Enterprise Server n'arrive pas à surveiller l'ordinateur exécutant DeviceLock Service en raison d'un nombre insuffisant de licences. DeviceLock Enterprise Server gère autant d'instances de DeviceLock Service qu'il y a de licences chargées dans DeviceLock Enterprise Server. Pour plus d'informations, veuillez consulter la section "License information" dans "Installation de DeviceLock Enterprise Server". L'icône d'ordinateur sera "ordinateur vert avec point d'exclamation. "

Les mêmes messages de statut (hormis **Computer is available**) sont également consignés dans le journal de surveillance, si bien que vous pouvez contrôler la situation des ordinateurs surveillés ultérieurement.

- **Last Scan Time**: la date et l'heure de la dernière tentative de scan. Cette tentative de scan peut être courronnée de success ou pas.
- **Last Successful Scan Time**: la date et l'heure de la dernière tentative de scan effectuée avec succès.
- **Service Uptime**: indique la durée pendant laquelle DeviceLock Service a fonctionné sur l'ordinateur surveillé.
- **Computer Uptime**: indique la durée pendant laquelle l'ordinateur a fonctionné. En comparant la durée de fonctionnement de l'ordinateur et la durée de service (voir ci-dessus), vous pouvez savoir en permanence si DeviceLock Service s'est arrêté de fonctionner ou pas en cours de session.
- **Service Version**: la version de DeviceLock Service. Les cinq derniers chiffres correspondent au numéro de fabrication.

Algorithme de surveillance

L'algorithme utilise dans le processus de surveillance est simple mais efficace:

1. Tout d'abord, DeviceLock Enterprise Server essaie de localiser l'ordinateur surveillé, afin de déterminer s'il fonctionne ou pas. S'il arrive à le localiser, l'ordinateur reçoit le statut **available** et la surveillance de l'ordinateur se poursuit. Sinon, il reçoit le statut **unavailable** et la surveillance de l'ordinateur cesse (l'événement est enregistré dans le journal de surveillance).
2. Puis, DeviceLock Enterprise Server essaie de se connecter à DeviceLock Service. S'il arrive à se connecter, DeviceLock Service reçoit le statut **available** et la surveillance de l'ordinateur se poursuit. Sinon, il reçoit le statut **unavailable** et la surveillance de l'ordinateur cesse (l'événement est enregistré dans le journal de surveillance).

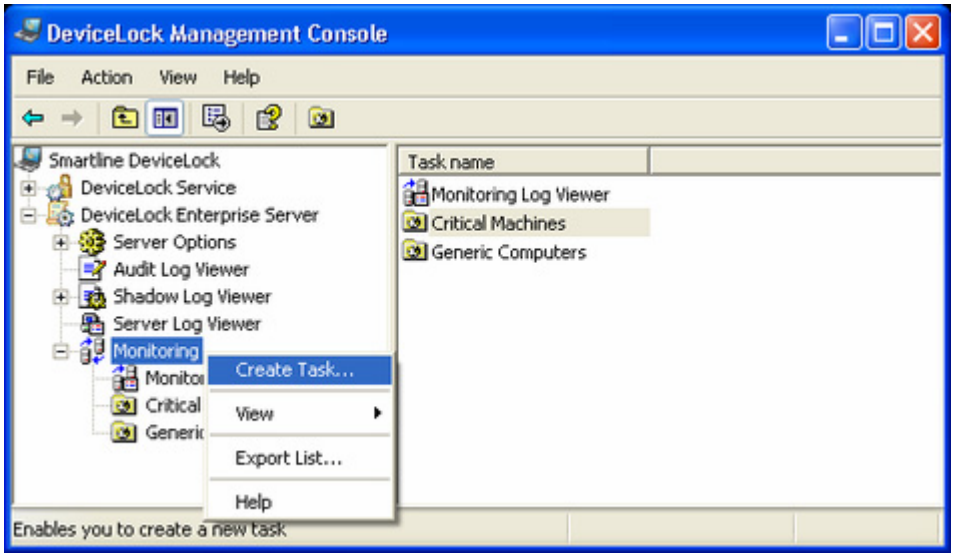
3. Si cette tâche vérifie l'intégrité de la politique de DeviceLock Service, la surveillance de l'ordinateur se poursuit. Sinon, la surveillance de l'ordinateur cesse (rien n'est enregistré dans le journal).
4. DeviceLock Enterprise Server télécharge la politique à partir de DeviceLock Service et la compare à la politique principale attribuée à cette tâche. S'il ne trouve pas de difference, la surveillance de l'ordinateur cesse (rien n'est enregistré dans le journal). S'il trouve une difference entre les deux politiques, la surveillance de l'ordinateur se poursuit (l'événement est enregistré dans le journal de surveillance).
5. Si cette tâche restaure la politique interrompue, DeviceLock Enterprise Server écrit la politique principale dans DeviceLock Service et la surveillance de l'ordinateur cesse (l'événement est enregistré dans le journal de surveillance). Sinon, la surveillance de l'ordinateur cesse (rien n'est enregistré dans le journal).

Si des erreurs se produisent à un niveau ou à un autre du processus ci-dessus, l'évènement correspondant est enregistrè dans le journal de surveillance. Si l'erreur en question n'est pas grave, la surveillance de l'ordinateur peut continuer. S'il s'agit d'une erreur grave, la surveillance de l'ordinateur cesse.

Certaines erreurs très graves (comme le «manque de mémoire») peuvent interrompre l'exécution de l'ensemble de la tâche.

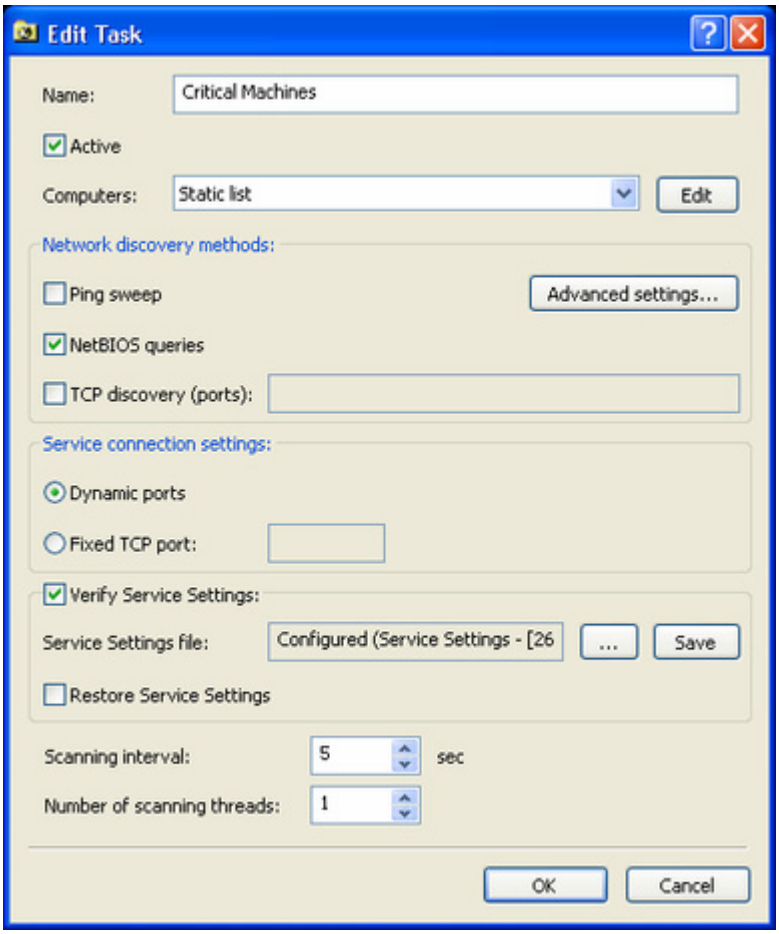
Créer / Modifier une tâche

Chaque tâche contient son propre groupe d'ordinateurs, d'actions et de paramètres de configuration.



Pour créer une nouvelle tâche, utilisez l'option **Create Task** du menu contextuel de l'élément **Monitoring**. Pour éditer une tâche existante, sélectionnez la tâche en question dans l'arborescence de gauche et utilisez l'option **Edit Task** du menu contextuel.

Pour supprimer définitivement la tâche, sélectionnez-la dans l'arborescence de gauche et utilisez l'option **Delete Task** du menu contextuel.



Name: le nom de la tâche utilisé pour identifier cette tâche dans la liste de tâches et dans le journal de surveillance.

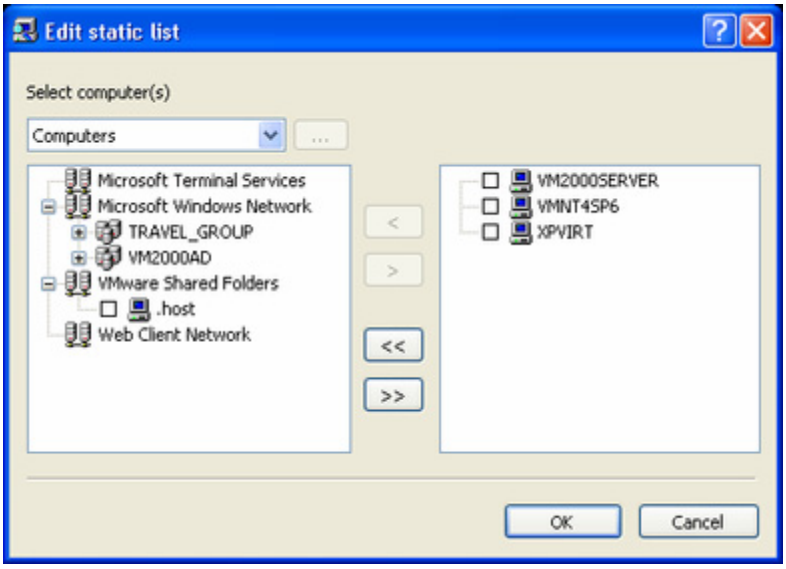
Active: le fait de cocher cette case permet à DeviceLock Enterprise Server d'exécuter la tâche considérée. Décochez-la pour désactiver la tâche sans la supprimer définitivement.

Computers: le type utilisé dans la liste des ordinateurs pour définir les ordinateurs qui seront surveillés par cette tâche.

Appuyez sur le bouton **Edit** pour configurer la liste sélectionnée dans **Computers**.

Deux types de listes d'ordinateurs sont pris en charge:

1. **Static list**: tous les ordinateurs sont spécifiés dans la liste par leurs noms ou leurs adresses IP. Comme cette liste est statique, même si certains ordinateurs ne figurent plus dans le réseau, ils seront surveillés (et les erreurs seront enregistrées) jusqu'à ce que leurs noms soient supprimés manuellement de la liste.



Les ordinateurs à surveiller doivent être indiqués dans la liste de droite. Vous devez sélectionner les ordinateurs necessaries dans la liste de gauche, puis les transférer dans la liste de droite en appuyant sur le bouton **>**.

Pour exclure certains ordinateurs du processus de surveillance, sélectionnez-les dans la liste de droite, puis appuyez sur le bouton **<**.

Les boutons **>>** et **<<** permettent d'ajouter et de supprimer tous les ordinateurs disponibles en même temps (inutile de sélectionner des ordinateurs dans la liste).

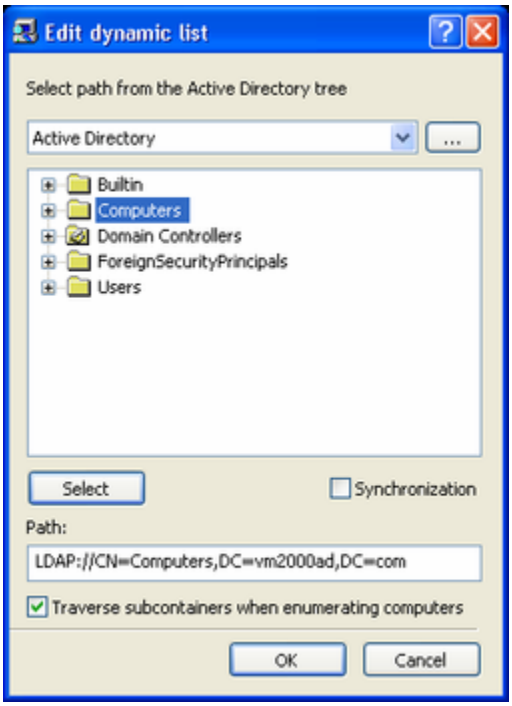
Il existe plusieurs méthodes flexibles de sélection des ordinateurs du réseau dans la liste de gauche:

- **Computers**: passez en revue l'arborescence du réseau et choisissez les ordinateurs qui vous intéressent
- **From File**: dans ce cas, chargez une liste d'ordinateurs prédéfinie à partir d'un fichier de texte externe puis sélectionnez les ordinateurs qui vous intéressent. Pour ouvrir un fichier externe, appuyez sur le bouton **...**. Un fichier de texte doit impérativement comporter le nom de chaque ordinateur ou son adresse IP sur des lignes séparées et peut être indifféremment en format Unicode ou non-Unicode.
- **Manual**: vous devez saisir les noms des ordinateurs manuellement pour les sélectionner. Chaque nom ou adresse IP d'ordinateur doit être saisi sur une ligne séparée.

2. **Dynamic list**: au lieu des noms ou des adresses IP des ordinateurs, la liste dynamique contient un chemin vers le dossier (p.ex. l'unité organisationnelle) dans l'arborescence du service de répertoire (de type Active Directory, Novell eDirectory, OpenLDAP, etc.). À chaque exécution de la tâche, DeviceLock Enterprise Server récupère tous les ordinateurs qui figurent dans ce dossier au moment considéré. Par conséquent, si un ordinateur a été supprimé de l'arborescence du répertoire, ou transféré dans un autre dossier, il ne sera plus surveillé. Et vice-versa, s'il y a un

nouvel ordinateur qui n'existait pas dans le dossier au moment où la tâche a été créée/modifiée, mais a été ajouté à ce dossier par la suite, il sera récupéré et surveillé au moment d'exécuter la tâche.

Remarque: Si DeviceLock Enterprise Server s'exécute sous Windows NT4, l'utilisation de la liste dynamique nécessite l'installation d'une Active Directory Extension. Vous pouvez la télécharger sur:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=7c219dcc-ec00-4c98-ba61-fd98467952a8



Un chemin vers le dossier à partir duquel les ordinateurs seront récupérés au moment d'exécuter la tâche doit être spécifié dans le paramètre **Path**. Utilisez la représentation de chaînes LDAP pour les noms distingués.

Vous pouvez explorer l'arborescence du répertoire et choisir le dossier nécessaire en appuyant sur le bouton **Select**. Dans ce cas, un chemin vers ce dossier sera indiqué automatiquement dans le paramètre **Path**.

Cochez la case **Traverse subcontainers when enumerating computers** pour permettre à DeviceLock Enterprise Server de récupérer les ordinateurs de tous les dossiers imbriqués dans le dossiers sélectionné. Sinon, tous les dossiers imbriqués sont ignorés, et seuls les ordinateurs situés directemnet dans le dossier sélectionné sont récupérés au moment d'exécuter la tâche.

Il y a deux façons d'utiliser le service de répertoire:

- **Active Directory**: Vous parcourez l'arborescence Active Directory et vous sélectionnez le dossier souhaité.
  Même si l'arborescence Active Directory peut aussi être affichée en choisissant l'option **LDAP** (voir ci-dessous), le mode Active Directory permet une meilleure efficacité entre le service de répertoire et le service DeviceLock Enterprise Server, d'où des économies de ressources.

Si vous devez fournir d'autres accréditations pour accéder à Active Directory, appuyez sur le bouton **...** pour ouvrir la boîte de dialogue **Credentials** et spécifier le compte d'utilisateur souhaité et son mot de passe correspondant.

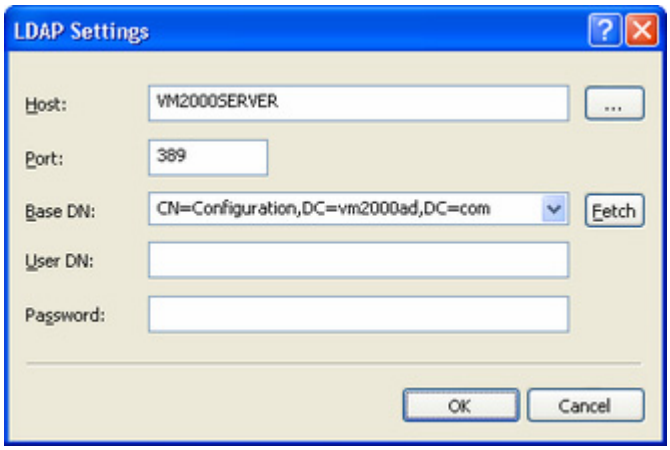
Remarque: Si aucune autre accréditation n'est spécifiée lors de l'accès à Active Directory, DeviceLock Enterprise Server utilise les accréditations du compte sous lequel son service a démarré. Pour plus d'informations, veuillez lire la description du paramètre Log on as.

Cochez la case **Synchronization** pour autoriser DeviceLock Enterprise Server à utiliser les mécanismes de synchronisation internes fournis par Active Directory. Cela réduira fortement la charge exercée sur le contrôleur de domaine et accélérera le processus de récupération des ordinateurs au moment d'exécuter la tâche.

Remarque: L'accès administrative à Active Directory est nécessaire pour utiliser la fonction de synchronisation.

- **LDAP**: Vous naviguez dans l'arborescence LDAP (Lightweight Directory Access Protocol, ou protocole d'accès au répertoire allégé) et sélectionnez le dossier souhaité.

  Pour configurer une connexion au serveur LDAP, appuyez sur le bouton **...** et ouvrez la boîte de dialogue **LDAP Settings**.



  Host: le nom ou l'adresse IP du serveur LDAP auquel il faut se connecter.

  Port: le port TCP/IP sur lequel le serveur LDAP accepte des connexions. Par défaut, il s'agit du port 389.

  Base DN: le point de départ de la navigation dans l'arborescence des répertoires. Utilisez la représentation de chaînes de LDAP pour les noms distingués (par exemple, cn=qa,o=SMARTLINE,c=US). Laissez le champ **Base DN** vierge pour commencer à naviguer depuis la racine.

  Appuyez sur le bouton **Fetch** pour obtenir tous les contextes d'attribution de noms publiés.

  User DN: le nom distingué (DN) de l'utilisateur de répertoire qui permet la connexion au répertoire. Utilisez la représentation de chaînes de LDAP pour les noms distingués (par exemple, cn=qa,o=SMARTLINE,c=US).

Remarque: Si aucun utilisateur n'est spécifié lors de l'accès à Active Directory, DeviceLock Enterprise Server utilise les accréditations du compte sous lequel son service a démarré. Pour plus d'informations, veuillez lire la description du paramètre Log on as.

Password: le mot de passe de l'utilisateur.

Network discovery methods: types d'exploration de réseau qui seront utilisés pour determiner le statut (**available** ou **unavailable**) des ordinateurs surveillés.

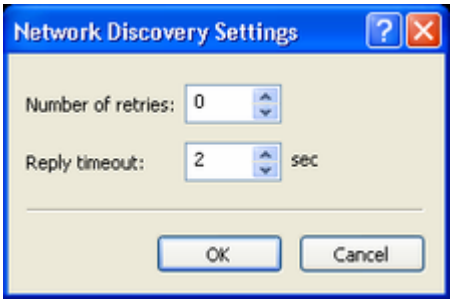
Lorsqu'il exécute cette tâche, DeviceLock Enterprise Server utilise toutes les méthodes de recherche sélectionnées dans l'ordre indiqué jusqu'à obtenir le statut **available** pour l'ordinateur cible. Si aucune des méthodes sélectionnées ne renvoie le statut **available**, l'ordinateur cible reçoit le statut **unavailable**.

Trois types d'exploration de réseau sont pris en charge:

1. **Ping sweep**: DeviceLock Enterprise Server envoie régulièrement un ping ICMP à l'ordinateur cible, puis attend sa réponse.
2. **NetBIOS queries**: si le Client for Microsoft Networks est installé sur l'ordinateur cible, cet ordinateur répondra à la demande de type NetBIOS envoyée par DeviceLock Enterprise Server.
3. **TCP discovery (ports)**: DeviceLock Enterprise Server vérifie la présence d'un port TCP ouvert particulier sur l'ordinateur cible. En utilisant la virgule (,) ou le point-virgule (;) en tant que séparateur, vous pouvez spécifier plusieurs ports, et ils seront vérifiés l'un après l'autre dans l'odre indiqué.

Remarque: Un pare-feu qui fonctionne sur un ordinateur cible peut bloquer l'envoi de tout ou partie des paquets de réseau, si bien qu'un tel ordinateur sera détecté comme unavailable (indisponible), même s'il est sous tension et actif.

Pour définir des paramètres supplémentaires pour les méthodes de recherche, appuyez sur le bouton **Advanced settings** et ouvrez la boîte de dialogue **Network Discovery Settings**.



Number of retries: le nombre de fois où DeviceLock Enterprise Server effectuera chaque type d'exploration tant qu'il renvoit le statut **unavailable**. 0 signifie qu'aucun nouvel essai n'aura lieu pour ce type d'exploration après le premier échec.

Reply timeout: la durée en secondes pendant laquelle DeviceLock Enterprise Server attendra effectivement une réponse de l'ordinateur cible pour chaque type d'exploration. Si DeviceLock Enterprise Server fonctionne sur un réseau lent ou encombré, vous risquez de devoir augmenter cette durée.

Service connection settings: ces options définissent la façon dont DeviceLock Enterprise Server devrait se connecter à DeviceLock Services sur les ordinataurs surveillés pour obtenir la version, les paramètes, etc. du service. Si les bons parameters de connexion ne sont pas specifies, DeviceLock Enterprise Server n'arrivera pas à se connecter aux services surveillés et leurs ordinateurs ne recevront pas le statut **available**.

Vous pouvez configurer DeviceLock Service pour qu'il utilise soit un port fixe, soit des ports dynamiques lors du processus d'installation. Pour plus d'informations sur le sujet, consultez les sections Installation automatique et Installation à distance via DeviceLock Enterprise Manager de ce manuel.

Il existe deux options de connexion:

- **Dynamic ports**: pour obliger DeviceLock Enterprise Server à utiliser des ports dynamiques pour les communications avec DeviceLock Service, sélectionnez cette option.
- **Fixed TCP port**: si DeviceLock Service est configuré pour accepter des connexions sur un port fixe, vous devez sélectionner cette option et spécifier ce numéro de port.

Remarque: Pour pouvoir se connecter aux DeviceLock Services surveillés et en obtenir les informations souhaitées, DeviceLock Enterprise Server doit disposer au moins de droits d'accès Read-only à ces services. Si cette tâche nécessite aussi d'enregistrer certains paramètres dans les DeviceLock Services surveillés, DeviceLock Enterprise Server doit disposer de droit Full access à ces services.

Pour se connecter aux DeviceLock Services surveillés, DeviceLock Enterprise Server utilise les accréditations du compte sous lequel son service a démarré. Il peut aussi utiliser une authentification par certificat DeviceLock si une clé privée est spécifiée. Pour plus d'informations, veuillez lire la description des paramètres Log on as et Certificate Name.

Verify Service Settings: cochez cette case si vous souhaitez verifier l'intégrité de la politique des DeviceLock Services exécutés sur les ordinateurs surveillés.

- **Service Settings file**: pour assigner la politique principale à la tâche, vous devez charger le fichier XML avec les paramètres de service (le ficher de politique principale). Le fichier de politique principale peut être créé sous DeviceLock Management Console, DeviceLock Group Policy Manager et/ou DeviceLock Service Settings Editor.

  Lors du processus de verification de politique, DeviceLock Enterprise Server télécharge la politique de chaque DeviceLock Service surveillé et la compare à la politique principale assignée à cette tâche.

  Tous les paramètres non configures (ceux qui ont le statut **Not Configured**) dans la politique principale sont ignores lors du processus de vérification de la politique. Cette fonction permet de surveiller l'intégrité des paramètres les plus importants uniquement et permet de changer les autres paramètres sans l'enregistrer dans le journal de surveillance.

  Pour charger le fichier de politique principale, appuyez sur le bouton **...**. Etant donné que la signature n'est pas validée à ce stade, il peut s'agir d'un fichier signé ou non

signé. Cependant, si vous chargez le fichier signé, son nom apparaîtra entre parenthèses dans le champ **Service Settings file**.

Si vous modifiez la tâche et que la politique principale est déjà assignée, vous pouvez l'exporter vers un fichier XML en appuyant sur le bouton **Save**.

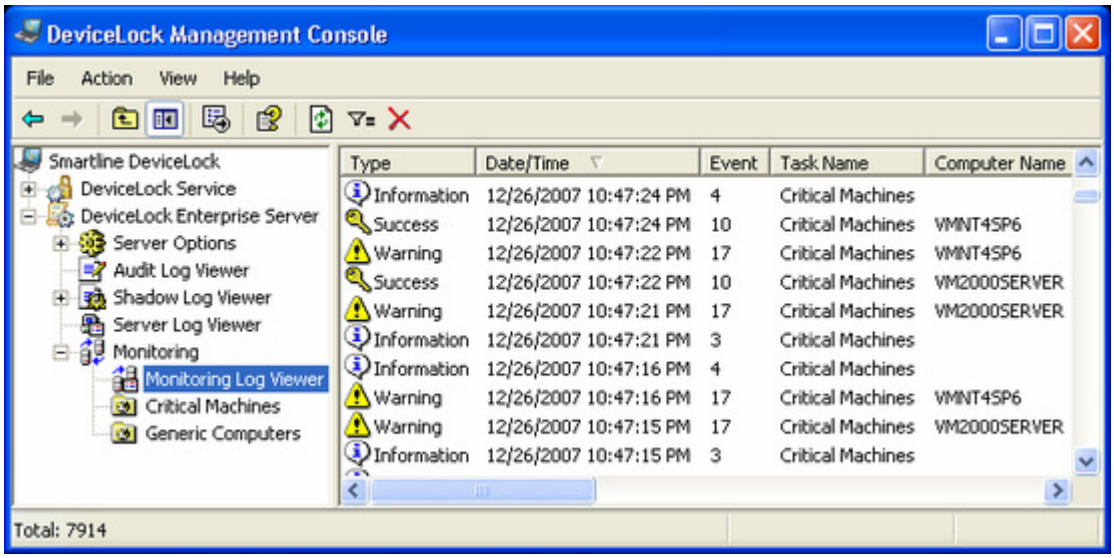
- **Restore Service Settings**: si cette case est cochée, DeviceLock Enterprise Server écrase la politique actuelle d'un DeviceLock Service surveillé pour lequel le processus de vérification de politique a échoué avec la politique principale assignée à cette tâche. Cette fonction permet non seulement de surveiller passivement l'intégrité de certains paramètres, mais aussi de les restaurer s'ils ont été modifiés.

Scanning interval: la durée en secondes qui doit s'écouler après la fin d'une tâche et avant que DeviceLock Enterprise Server ne commence à exécuter à nouveau la même tâche.

Number of scanning threads: le nombre maximum de traitements qui peuvent être utilisés par cette tâche de façon simultanée. Vous pouvez augmenter ce nombre de façon à mener plusieurs explorations d'ordinateurs de front. Cependant, plus le nombre de traitements augmente, plus il faut disposer de ressources (notamment en termes de mémoire RAM et de bande passante réseau) au niveau du DeviceLock Enterprise Server.

Monitoring Log Viewer (Module de visualisation du journal de surveillance)

Ce module de visualisation permet de récupérer le journal de surveillance. Le journal de surveillance est utilise par les tâches pour enregistrer les informations sur les ordinateurs surveillés et les DeviceLock Services.


DeviceLock Management Console
File Action View Help
Smartline DeviceLock
DeviceLock Service
DeviceLock Enterprise Server
Server Options
Audit Log Viewer
Shadow Log Viewer
Server Log Viewer
Monitoring
Monitoring Log Viewer
Critical Machines
Generic Computers
Type Date/Time Event Task Name Computer Name
Information 12/26/2007 10:47:24 PM 4 Critical Machines
Success 12/26/2007 10:47:24 PM 10 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:22 PM 17 Critical Machines VMNT4SP6
Success 12/26/2007 10:47:22 PM 10 Critical Machines VM2000SERVER
Warning 12/26/2007 10:47:21 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:21 PM 3 Critical Machines
Information 12/26/2007 10:47:16 PM 4 Critical Machines
Warning 12/26/2007 10:47:16 PM 17 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:15 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:15 PM 3 Critical Machines
Total: 7914

Les colonnes de ce module de visualisation sont les suivantes:

- **Type**: la classe de l'événement: **Success**, **Information**, **Warning** ou **Error**.
- **Date/Time**: la date et l'heure de l'événement.

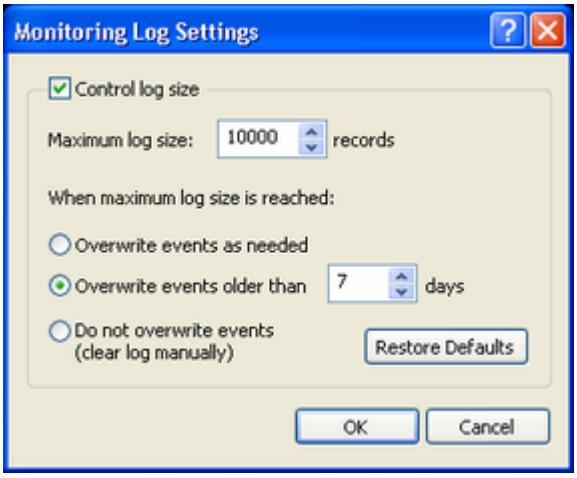
- **Event**: un numéro qui identifie le type d'événement considéré.
- **Task Name**: le nom de la tâche responsable de cet événement. Peut être vide si un événement n'est lié à aucune tâche.
- **Computer Name**: le nom de l'ordinateur appurtenant à la tâche qui est responsable de cet événement. Peut être vide si un événement n'est pas lié à l'ordinateur.
- **Information**: information liée à l'événement, comme le statut, une erreur, un avertissement, etc.
- **Server**: le nom du serveur sur lequel s'est produit l'événement.
- **Record N**: le numéro de l'enregistrement.

Pour mettre à jour la liste, sélectionnez l'élément **Refresh** du menu contextuel disponible en cliquant droit ou utilisez le bouton approprié de la barre d'outils.

Pour supprimer tous les événements de ce journal, sélectionnez l'option **Clear** du menu contextuel ou utilisez le bouton approprié de la barre d'outils.

Paramètres du journal de surveillance

Pour définir une taille maximale de journal et spécifier ce que DeviceLock Enterprise Server doit faire si le journal de surveillance est plein, utilisez les **Settings** du menu contextuel du Monitoring Log Viewer.

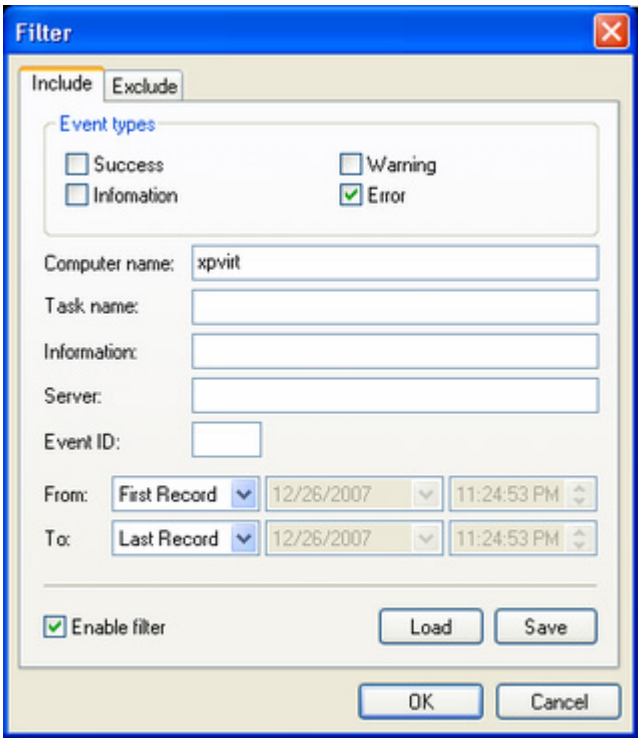


Pour plus d'informations sur ces paramètres, veuillez vous reporter à la section Paramètres du journal d'audit (serveur) de ce manuel.

Filtre du journal de surveillance

Les données du module de visualisation du journal de surveillance peuvent être filtrées afin de ne voir que les enregistrements qui répondent aux critères indiqués.

Pour ouvrir la boîte de dialogue **Filter**, utilisez l'option **Filter** du menu contextuel du Monitoring Log Viewer, ou utilisez le bouton approprié de la barre d'outils.



Il n'y a que peu de différences entre la définition des filtres du journal d'audit et celle des filtres du journal de surveillance: consultez donc tout d'abord le chapitre Filtre de journal d'audit (service) de ce manuel.

Lorsque le filtre est actif, vous pouvez le définir en saisissant des valeurs dans les champs suivants:

- **Success** – indique s'il faut filtrer ou non les èvènements de la catègorie **Success**.
- **Information** – indique s'il faut filtrer ou non les événements de la catégorie **Information**.
- **Warning** – indique s'il faut filtrer ou non les èvènements de la catègorie **Warning**.
- **Error** – indique s'il faut filtrer ou non les événements de la catégorie **Error**.
- **Computer Name** – le texte qui correspond à une valeur de la colonne **Computer Name** du Monitoring Log Viewer. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Task Name** – le texte qui correspond à une valeur de la colonne **Task Name** du Monitoring Log Viewer. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).

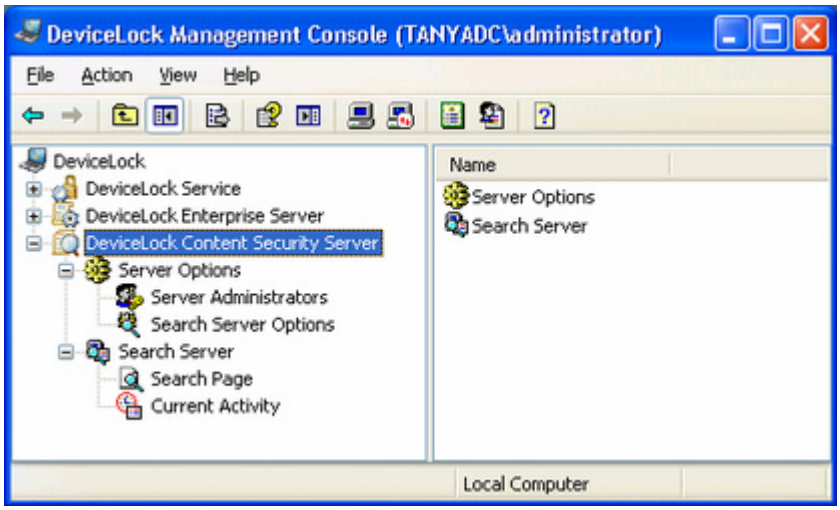
- **Information** – le texte qui correspond à une valeur de la colonne **Information** du Monitoring Log Viewer. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Server** – le texte qui correspond à une valeur de la colonne **Server** du Monitoring Log Viewer. Ce champ n'est pas sensible à la casse et vous pouvez utiliser des jokers.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **Event ID** – le texte qui correspond à une valeur de la colonne **Event** du Monitoring Log Viewer.
  Vous pouvez saisir plusieurs valeurs, séparées par un point-virgule (;).
- **From** – indique le dèbut de la pèriode qui contient les èlèments que vous voulez filtrer. Sèlectionnez **First Event** pour voir les èvènements en commençant par le premier enregistrement du journal. Sèlectionnez **Events On** pour voir les èvènements ayant eu lieu à partir d'une date et d'une heure donnèes.
- **To** – indique la fin de la pèriode qui contient les èvènements que vous voulez voir. Sèlectionnez **Last Event** pour voir les èvènements en terminant par le dernier enregistrement du journal. Sèlectionnez **Events On** pour voir les èvènements ayant eu lieu jusqu'à une date et une heure donnèes.

Gestion et utilisation de DeviceLock Content Security Server

Parcourir DeviceLock Content Security Server

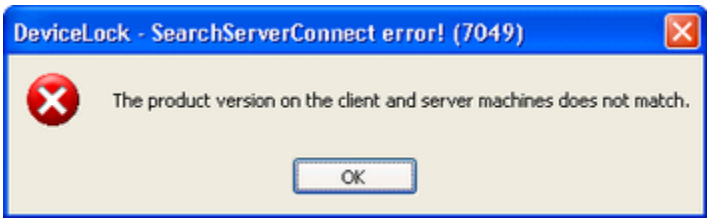
Avant de découvrir les fonctionnalités de DeviceLock Content Security Server, examinons les principales règles de navigation de ce programme.

Utilisez le module **DeviceLock Content Security Server** de DeviceLock Management Console pour configurer et utiliser DeviceLock Content Security Server.



Cliquez droit sur le module DeviceLock Content Security Server pour afficher les instructions suivantes:

- **Connect**: permet la connexion à l'ordinateur exécutant DeviceLock Content Security Server. Pour en savoir plus, consultez la section «Connexion aux ordinateurs.»
  En cas de connexion à un ordinateur équipé d'une ancienne version de DeviceLock Content Security Server, il se peut que le message suivant apparaisse:

  Dans ce cas, vous devez installer la nouvelle version de DeviceLock Content Security Server sur cet ordinateur. Pour en savoir plus sur la façon d'installer DeviceLock Content Security Server, consultez la section «Installation de DeviceLock Content Security Server.»

- **Reconnect**: renouvelle la connexion à l'ordinateur actuellement connecté.
- **Connect to Last used Server at Startup**: cochez cette option pour ordonner à DeviceLock Management Console de se connecter automatiquement au dernier serveur utilisé à chaque démarrage.
- **Certificate Generation Tool**: lance l'outil spécial qui permet de générer des DeviceLock Certificates. Pour en savoir plus, consultez la section «Création de DeviceLock Certificates.»
- **DeviceLock Signing Tool**: exécute l'outil spécial qui permet d'accorder aux utilisateurs un accès temporaire aux périphériques demandés et de signer les fichiers XML avec des paramètres DeviceLock Service. Pour en savoir plus, consultez la section «DeviceLock Signing Tool.»
- **About DeviceLock**: ouvre une boîte de dialogue contenant des informations sur la version de DeviceLock employée et sur vos licences.

Développez le module **DeviceLock Content Security Server** pour afficher les instructions suivantes:

- Le module **Server Options**. Utilisez ce module pour configurer DeviceLock Content Security Server et Search Server.
  La liste suivante décrit les paramètres généraux que vous pouvez configurer pour DeviceLock Content Security Server:
  - **Server Administrators**: Utilisez ce paramètres pour spécifier les membres du groupe Server Administrator et leurs droits d'accès.
  - **DeviceLock certificate**: Utilisez ce paramètre pour installer ou supprimer un DeviceLock Certificate.

- **Service startup account**: Utilisez ce paramètre pour spécifier les informations de compte au démarrage, comme le nom de compte et le mot de passe du serveur.
- **TCP port**: Utilisez ce paramètre pour spécifier le port TCP utilisé par le serveur pour se connecter à DeviceLock Management Console.

La liste suivante décrit les paramètres de recherche systématique configurables pour Search Server:

- **DeviceLock Enterprise Server(s)**: Utilisez ce paramètre pour préciser le ou les DeviceLock Enterprise Server(s) dont les données seront indexées pour une recherche systématique.
- **Index directory**: Utilisez ce paramètre pour spécifier l'emplacement de l'indice systématique de texte.
- **Indexing interval**: Utilisez ce paramètre pour préciser l'intervalle de temps, en minutes, entre la fin d'un processus d'indexation et le début du processus d'indexation suivant.
- **Merge Interval**: Utilisez ce paramètre pour préciser l'intervalle de temps, en minutes, au bout duquel les opérations de fusion seront effectuées.
- **Extract text from binary**: Utilisez ce paramètre pour autoriser ou interdire la présence de textes en provenance des données binaires dans l'indice.
- **Search Server License(s)**: Utilisez ce paramètre pour installer le nombre de licences Seach Server requis.

- Le module **Search Server**. Utilisez ce module pour effectuer une recherche et surveiller l'activité d'indexation actuelle.

Configuration des paramètres généraux de DeviceLock Content Security Server

DeviceLock Content Security Server comporte deux types de paramètres de configuration:

- **Paramètres généraux de DeviceLock Content Security Server.** Ces paramètres affectent le déploiement de DeviceLock Content Security Server dans son ensemble.
- **Paramètres de recherche systématique de Search Server.** Ces paramètres sont liés à la recherche systématique et n'affectent que le composant Search Server de DeviceLock Content Security Server. Pour en savoir plus, consultez la section «Configuration des paramètres de recherche systématique de Search Server.»

Il est possible de configurer les paramètres de serveur généraux lors de l'installation initiale de DeviceLock Content Security Server, ou bien d'utiliser DeviceLock Management Console pour les configurer et/ou les modifier une fois le serveur installé et activé.

Remarque: Pour pouvoir gérer et utiliser DeviceLock Content Security Server, il convient d'être membre du groupe Server Administrators et de disposer de droits suffisants.

Avant de pouvoir utiliser la DeviceLock Management Console, il convient de la connecter à l'ordinateur sur lequel DeviceLock Content Security Server est installé et en cours d'exécution. Pour ce faire,

cliquez droit sur l'option **DeviceLock Content Security Server** de l'arborescence de console, puis sur **Connect**. Pour en savoir plus, consultez la section «Connexion aux ordinateurs.»

DeviceLock Management Console permet d'effectuer les tâches de configuration suivantes:

- Configuration des utilisateurs ayant accès à DeviceLock Content Security Server.
- Modification des informations de compte de démarrage, comme le nom ou le mot de passe du compte, pour le service DeviceLock Content Security Server.
- Installation ou suppression du DeviceLock Certificate utilisé pour authentifier les communications entre DeviceLock Content Security Server et DeviceLock Enterprise Server.
- Changement du port TCP utilisé par DeviceLock Content Security Server pour la connexion à DeviceLock Management Console.

Ces tâches peuvent être effectuées de façon individuelle ou collective.

Pour effectuer les tâches de façon collective, il est possible d'utiliser l'assistant DeviceLock Content Security Server. Il s'agit de l'assistant qui démarre automatiquement lors de l'installation ou de la mise à niveau de DeviceLock Content Security Server.

Pour effectuer les tâches de configuration de façon collective

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, cliquez droit sur **Server Options**, puis sur **Properties**.

   La première page de l'assistant apparaît.

3. Parcourez l'assistant. A la fin de chaque page, passez à la suivante en cliquant sur **Next**, ou à la précédante en cliquant sur **Back**. Une fois la dernière page atteinte, cliquez sur **Finish** pour refermer l'assistant.

   Pour en savoir plus sur la façon d'installer DeviceLock Content Security Server à l'aide de l'assistant de configuration, consultez la section «Installation de DeviceLock Content Security Server.»

On trouvera ci-dessous des instructions détaillées sur la façon d'effectuer les tâches de configuration individuelles à l'aide de DeviceLock Management Console.

Tâche: Configuration des utilisateurs ayant accès à DeviceLock Content Security Server

Vous pouvez sélectionner les utilisateurs autorisés à accéder à votre DeviceLock Content Security Server. Le serveur est ainsi moins accessible aux intrus et donc moins exposé.

Pour choisir les utilisateurs autorisés à accéder au serveur

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, effectuez l'une ou l'autre des actions suivantes:

- Sélectionnez **Server Options**. Dans le panneau d'affichage détaillé, double-cliquez sur **Server Administrators** ou cliquez droit sur **Server Administrators** puis sur **Properties**.

  Lorsque vous sélectionnez des Server Options dans l'arborescence, celles-ci s'affichent dans le panneau d'affichage détaillé.

  - OU –
- Développez **Server Options**. Dans **Server Options**, cliquez droit sur **Server Administrators** puis cliquez sur **Properties**.

La boîte de dialogue DeviceLock Content Security Server apparaît.

3. Dans la boîte de dialogue **DeviceLock Content Security Server**, procédez comme suit:

ACTION	PROCEDURE
Activer la sécurité par défaut	• Cochez la case **Enable Default Security**. *Si la sécurité par défaut est activée, les utilisateurs qui sont membres du groupe local Administrators bénéficient d'un accès complet à DeviceLock Content Security Server*.
Limiter l'accès au serveur à des utilisateurs particuliers	1. Décochez la case **Enable Default Security**. 2. Dans **Users**, cliquez sur **Add** pour ajouter les utilisateurs spécifiques autorisés à accéder à DeviceLock Content Security Server. *La boîte de dialogue Select Users or Groups apparaît*. 3. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes sélectionnés sont ajoutés au groupe Server Administrators et affichés dans le champ Users de la boîte de dialogue DeviceLock Content Security Server. Les Server Administrators sont des utilisateurs ou des groupes autorisés à effectuer des tâches liées à la configuration et à l'utilisation de DeviceLock Content Security Server. Par défaut, les membres du groupe Server Administrators disposent de droits d'accès complets au serveur*. Pour modifier leurs droits d'accès, dans **Users**, sélectionnez l'utilisateur ou le groupe puis cliquez sur n'importe quelle option de la liste des droits d'accès. Les options disponibles sont les suivantes: **Full Access:** permet l'accès complet à DeviceLock Content Security Server. Les utilisateurs peuvent installer/désinstaller DeviceLock Content Security Server, s'y connecter à l'aide de DeviceLock Management Console, modifier les paramètres et effectuer des recherches. **Change:** permet d'accéder à DeviceLock Content Security Server en mode modification. Les utilisateurs peuvent installer/désinstaller DeviceLock Content Security Server, s'y connecter à l'aide de DeviceLock Management Console, modifier les paramètres et effectuer des recherches. Mais ils ne peuvent pas ajouter ni supprimer des utilisateurs au/du groupe Server Administrators, ni modifier les droits d'accès accordés aux Server Administrators. **Read-only:** permet l'accès en lecture seule à DeviceLock Content Security Server. Les utilisateurs peuvent se connecter à DeviceLock Content Security Server à l'aide de DeviceLock Management Console, effectuer des recherches et afficher les paramètres. Mais ils

ACTION	PROCEDURE
	ne peuvent pas modifier des paramètres ou créer un nouvel indice de Search Server. **Remarque:** Nous recommandons fortement d'accorder des privilèges d'administrateurs locaux aux membres du groupe Servers Administrators. Pour supprimer un utilisateur ou un groupe du groupe Server Administrators, sélectionnez l'utilisateur ou le groupe en question dans **Users**, puis cliquez sur **Delete**. *Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*.

4. Cliquez sur **OK**.

Tâche: Changement de compte ou de mot de passe de démarrage du service

Avec le temps, il peut s'avérer nécessaire de changer le compte de démarrage de DeviceLock Content Security Server défini lors du processus d'installation. Il est aussi possible de changer le mot de passe du compte de démarrage du service.

Pour changer le compte ou le mot de passe de démarrage du service

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, sélectionnez **Server Options**.

   Lorsque vous sélectionnez des Server Options dans l'arborescence, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **Service startup account** ou cliquez droit sur **Service startup account** puis sur **Properties**.

   La boîte de dialogue DeviceLock Content Security Server apparaît.

4. Dans la boîte de dialogue **DeviceLock Content Security Server**, procédez comme suit:

ACTION	PROCEDURE
Changer le compte de démarrage du service	1. Dans le champ **Log on as**, cliquez sur **Browse**. *La boîte de dialogue Select User apparaît*. 2. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select User**, saisissez le nom de l'utilisateur, puis cliquez sur **OK**. *L'utilisateur sélectionné s'affiche dans le champ This account de la boîte de dialogue DeviceLock Content Security Server*. *Il est conseillé d'utiliser un compte comportant des privilèges d'administration sur tous les ordinateurs exécutant DeviceLock Enterprise Server. Dans un environnement de domaine, il est conseillé d'utiliser un compte faisant partie du groupe Domain Admins. Sinon, il faut utiliser l'identification par DeviceLock Certificate*.

ACTION	PROCEDURE
Modifier le mot de passe du compte de service	1. Saisissez un nouveau mot de passe dans le champ **Log on as** de la boîte de dialogue **Password**. 2. Saisissez à nouveau votre nouveau mot de passe dans la boîte de dialogue **Confirm password**.
Affecter le compte Local System au serveur	• Dans le champ **Log on as**, cliquez sur **Local System account**. *Si le service utilise ce compte, il ne peut pas accéder au DeviceLock Enterprise Server qui fonctionne sur un ordinateur distant et doit utiliser le DeviceLock Certificate pour s'y identifier*.

5. Cliquez sur **OK**.

Tâche: Installation ou suppression du DeviceLock Certificate utilisé pour authentifier les communications entre DeviceLock Content Security Server et DeviceLock Enterprise Server

Dans certains cas, le compte d'utilisateur dans lequel DeviceLock Content Security Server fonctionne ne peut pas accéder au DeviceLock Enterprise Server distant. Dans ces cas, vous pouvez utiliser l'identification par DeviceLock Certificate. Pour ce faire, installez la même clé privée de DeviceLock Certificate sur DeviceLock Content Security Server et DeviceLock Enterprise Server. Pour des informations détaillées sur les DeviceLock Certificates, consultez le chapitre «DeviceLock Certificates.»

Pour installer ou supprimer DeviceLock Certificate sur DeviceLock Content Security Server

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, sélectionnez **Server Options**.

   Lorsque vous sélectionnez des Server Options dans l'arborescence, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **DeviceLock certificate** ou cliquez droit sur **DeviceLock certificate** puis sur **Properties**.

   La boîte de dialogue DeviceLock Content Security Server apparaît.

4. Dans la boîte de dialogue **DeviceLock Content Security Server**, procédez comme suit:

ACTION	PROCEDURE
Installer la clé privée de DeviceLock Certificate	1. En regard du champ **Certificate Name**, cliquez sur le bouton pour ouvrir la boîte de dialogue **Select the DeviceLock Certificate file** et naviguer jusqu'au fichier à utiliser. 2. Dans la liste **Look in** de la boîte de dialogue **Select the DeviceLock Certificate file**, cliquez sur l'emplacement qui contient le certificat. 3. Dans la liste des dossiers, identifiez et ouvrez le dossier qui

ACTION	PROCEDURE
	contient le certificat. 4. Cliquez sur le fichier, puis sur **Open**. *Le nom de certificat apparaît désormais dans le champ Certificate Name de la boîte de dialogue DeviceLock Content Security Server*.
Supprimer la clé privée de DeviceLock Certificate	• En regard du champ **Certificate Name**, cliquez sur **Remove**.

5. Cliquez sur **OK**.

Tâche: Changement du port TCP utilisé pour se connecter à DeviceLock Management Console

A terme, il peut s'avérer nécessaire de changer le port TCP utilisé par DeviceLock Content Security Server pour se connecter à DeviceLock Management Console.

Pour changer le port TCP utilisé pour se connecter à DeviceLock Management Console

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, sélectionnez **Server Options**.

   Lorsque vous sélectionnez des Server Options dans l'arborescence, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **TCP port** ou cliquez droit sur **TCP port** puis sur **Properties**.

   La boîte de dialogue DeviceLock Content Security Server apparaît.

4. Dans le champ **Connection Settings** de la boîte de dialogue **DeviceLock Content Security Server**, effectuez l'une des actions suivantes:
   - Cliquez sur **Dynamic ports** pour obliger DeviceLock Content Security Server à utiliser un port dynamique.
     - OU -
   - Cliquez sur **Fixed TCP port** pour obliger DeviceLock Content Security Server à utiliser un port statique. Puis, saisissez le numéro de port dans le champ **Fixed TCP port**.
     Par défaut, DeviceLock Content Security Server utilise le port TCP 9134.
5. Cliquez sur **OK**.

Configuration des paramètres de recherche systématique de texte pour Search Server

Les paramètres de recherche systématique de texte sont liés à la recherche systématique et n'affectent que l'élément Search Server de DeviceLock Content Security Server.

L'installation de DeviceLock Content Security Server ne permet d'installer que les licences Search Server. Utilisez DeviceLock Management Console pour définir l'ensemble des options de configuration de Search Server.

DeviceLock Management Console permet d'effectuer les tâches de configuration suivantes:

- Installer le nombre de licences Search Server requis.
- Préciser les DeviceLock Enterprise Servers dont les données doivent être indexées pour la recherche systématique de texte.
- Préciser l'emplacement de l'indice systématique de texte.
- Permettre ou interdire l'inclusion d'informations textuelles en provenance des données binaires dans l'indice.
- Configurer le programme d'indexation systématique du texte.
- Configurer un programme pour les opérations de fusion.
- Reconstruire instantanément l'indice systématique de texte.
- Mettre à jour instantanément l'indice existant.
- Surveiller et mettre à jour le statut de l'activité d'indexation en cours.

Tâche: Installer le nombre de licences Search Server requis

L'utilisation de DeviceLock Content Security Server nécessite l'achat d'une licence Search Server spéciale. Vous pouvez utiliser la même licence sur un nombre illimité d'ordinateurs exécutant DeviceLock Content Security Server.

Le modèle de gestion de licence de Search Server dépend du nombre d'entrées de journal à indexer pour la recherche de texte systématique. Chaque licence permet à Search Server d'indexer 1000 entrées des journaux de réplication (journal de réplication et journal de réplication supprimé), et 5000 entrées de chacun des autres journaux (journal d'audit, journal de serveur et journal de surveillance).

En fonction du nombre réel d'entrées de journal sur vos DeviceLock Enterprise Servers, vous pouvez acheter le nombre de licences de votre choix. Si vous utilisez plusieurs licences Search Server, le nombre d'entrées de journal indexables est la somme de celles correspondant à chaque licence. La période d'essai de DeviceLock Content Security Server est de 30 jours. Pendant la période d'essai, Search Server peut indexer 2000 entrées à partir des journaux de réplication et 10 000 entrées à partir des autres journaux. Il est toujours possible d'acheter et d'installer des licences Search Server supplémentaires.

Pour installer des licences Search Server

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **Search Server License(s)** ou cliquez droit sur **Search Server License(s)** puis sur **Properties**.

   La boîte de dialogue DeviceLock Content Security Server apparaît.

4. Dans la boîte de dialogue **DeviceLock Content Security Server**, cliquez sur **Load License(s)** pour parcourir le fichier de licence.
5. Dans la liste **Look in** de la boîte de dialogue **Select the DeviceLock license file**, cliquez sur l'emplacement qui contient le fichier de licence.
6. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier de licence.
7. Cliquez sur le fichier, puis sur **Open**.

   Les informations sur les fichiers de licence installés figurent dans le champ «Licence information» de la boîte de dialogue DeviceLock Content Security Server.

   Le nombre de licences qu'il est possible d'installer n'est pas limité et dépend des besoins de votre entreprise. Les licences supplémentaires doivent être ajoutées une par une.

8. Cliquez sur **OK**.

Tâche: Préciser les DeviceLock Enterprise Servers dont les données doivent être indexées pour la recherche systématique de texte

Pour lancer le processus de création d'indice systématique de texte, il faut préciser les DeviceLock Enterprise Servers dont les données doivent être indexées. Search Server démarre le processus d'indexation automatiquement dès que vous choisissez un ou plusieurs DeviceLock Enterprise Servers.

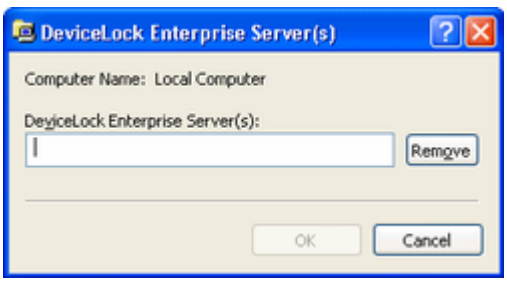
Pour choisir des DeviceLock Enterprise Servers

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **DeviceLock Enterprise Server(s)** ou cliquez droit sur **DeviceLock Enterprise Server(s)** puis sur **Properties**.

   La boîte de dialogue DeviceLock Enterprise Server(s) apparaît.



4. Dans la boîte de dialogue **DeviceLock Enterprise Server(s)**, saisissez l'adresse IP ou le nom de l'ordinateur qui exécute DeviceLock Enterprise Server.

   Les différents noms d'ordinateurs ou adresses IP doivent être séparés par un point-virgule (;).

   Remarque: Vérifiez que DeviceLock Enterprise Server est bien installé et accessible à DeviceLock Content Security Server, sinon ses données ne seront pas indexées par Search Server.

   Pour supprimer des noms d'ordinateurs ou des adresses IP, cliquez sur **Remove**.

5. Cliquez sur **OK**.

Tâche: Préciser l'emplacement de l'indice systématique de texte

Vous pouvez préciser l'emplacement de l'indice systématique de texte. Sinon, l'indice systématique de texte est créé dans le répertoire par défaut ***%ProgramFiles%\DeviceLock Content Security Server\Index***. Search Server lance le processus d'indexation automatiquement à chaque fois que vous indiquez un emplacement différent.

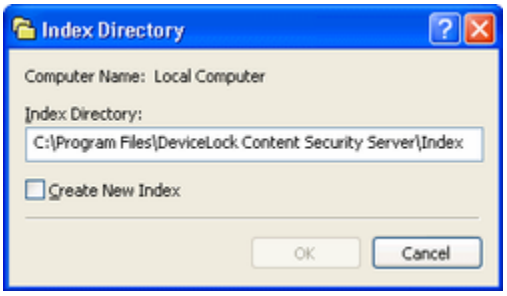
Pour préciser l'emplacement de l'indice

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **Index directory** ou cliquez droit sur **Index directory** puis sur **Properties**.

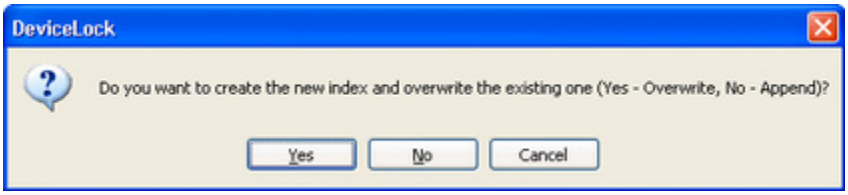
   La boîte de dialogue Index Directory apparaît.



4. Dans le champ **Index Directory** de la boîte de dialogue **Index Directory**, saisissez le chemin que vous souhaitez utiliser en tant qu'emplacement de l'indice par défaut.

   Pour créer instantanément un nouvel indice, cochez la case **Create New Index**.

   Si l'indice existe déjà à l'emplacement indiqué et que vous choisissez de créer un nouvel indice, le champ de message suivant s'affiche:



Dans le champ de message, cliquez sur **Yes** pour recréer complètement et instantanément l'indice systématique de texte. Cliquez sur **No** pour mettre à jour instantanément l'indice systématique de texte.

5. Cliquez sur **OK**.

Tâche: Permettre ou interdire l'inclusion d'informations de texte en provenance des données binaires dans l'indice

Il est possible de permettre ou d'interdire l'inclusion d'informations de texte en provenance des données binaires dans l'indice.

Pour activer ou désactiver l'extraction de texte en provenance des données binaires

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **Extract text from binary** ou cliquez droit sur **Extract text from binary**, puis sur **Enable** ou **Disable**.

Tâche: Configurer le programme d'indexation systématique du texte

L'indexation systématique du texte permet la création et la mise à jour postérieure de l'indice systématique du texte.

Il est possible de programmer le processus d'indexation afin qu'il démarre automatiquement au bout d'un certain temps. Le programme d'indexation systématique du texte est configuré en fonction de l'intervalle d'indexation. L'intervalle d'indexation sert à préciser l'intervalle de temps, en minutes, entre la fin d'un processus d'indexation et le début du processus d'indexation suivant. Par défaut, l'intervalle d'indexation est de 60 minutes.

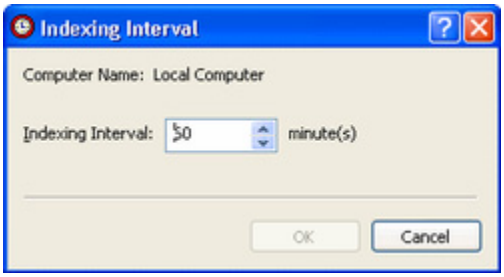
Pour configurer le programme d'indexation systématique du texte

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.

3. Dans le panneau d'affichage détaillé, double-cliquez sur **Indexing interval** ou cliquez droit sur **Indexing interval** puis sur **Properties**.

   La boîte de dialogue Indexing Interval apparaît.



4. Dans le champ **Indexing Interval** de la boîte de dialogue **Indexing Interval**, saisissez ou sélectionnez le nombre de minutes de l'intervalle d'indexation.
5. Cliquez sur **OK**.

Tâche: Configurer un programme pour les opérations de fusion.

Les opérations de fusion servent à combiner les indices temporaires sous forme d'indice principal permanent utilisé pour les recherches. Il est possible de programmer le processus de fusion afin qu'il démarre automatiquement au bout d'un certain temps. Le programme est configuré en fonction de l'intervalle de temps de fusion. L'intervalle de temps de fusion détermine la fréquence, en minutes, de consolidation des indices temporaires sous forme d'indice principal permanent par Search Server. En d'autres termes, il détermine à quelle fréquence Search Server met à jour l'indice principal permanent avec de nouvelles données lors d'une opération d'indexation. Par défaut, la fusion est effectuée toutes les 10 minutes. Vous pouvez spécifier une valeur entre 1 et 1 000 000.

Prenez les éléments suivants en considération lorsque vous indiquez une valeur:

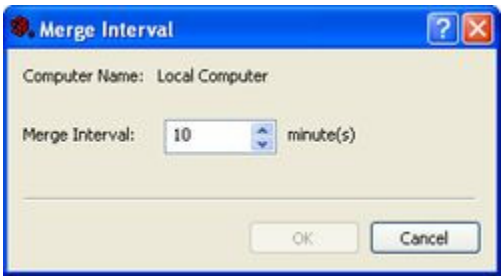
- Un petit intervalle de temps de fusion correspond à des mises à jour fréquentes de l'indice principal.
- La recherche systématique de texte n'est pas possible lorsqu'une fusion est en cours.

Pour configurer un programme pour les opérations de fusion

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Server Options**.
2. Dans **Server Options**, sélectionnez **Search Server Options**.

   Lorsque vous sélectionnez Search Server Options dans l'arborescence de console, celles-ci s'affichent dans le panneau d'affichage détaillé.
3. Dans le panneau d'affichage détaillé, double-cliquez sur **Merge Interval** ou cliquez droit sur **Merge Interval** puis sur **Properties**.

   La boîte de dialogue Merge Interval apparaît.



4. Dans le champ **Merge Interval** de la boîte de dialogue **Merge Interval**, saisissez ou sélectionnez le nombre de minutes de l'intervalle de fusion.
5. Cliquez sur **OK**.

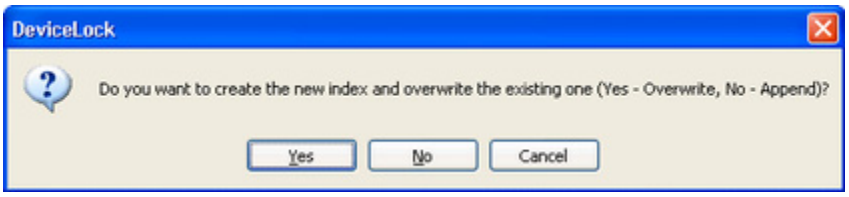
Tâche: Recréer instantanément l'indice systématique de texte

Il est possible de recréer instantanément l'indice systématique de texte.

Pour recréer instantanément l'indice systématique de texte

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans DeviceLock Content Security Server, cliquez droit sur **Search Server**, puis sur **Create New Index**.

   Si l'indice existe déjà et que vous choisissez de créer un nouvel indice, le champ de message suivant s'affiche:



   Dans le champ de message, cliquez sur **Yes** pour recréer complètement et instantanément l'indice systématique de texte. Cliquez sur **No** pour mettre à jour instantanément l'indice systématique de texte.

Tâche: Mettre à jour instantanément l'indice existant

Si de nouvelles données sont ajoutées à DeviceLock Enterprise Server et que vous souhaitez mettre à jour instantanément l'indice systématique de texte existant à l'aide de ces données, procédez comme suit :

Pour mettre à jour instantanément l'indice existant

1. Dans l'arborescence, développez **DeviceLock Content Security Server**.
2. Dans **DeviceLock Content Security Server**, cliquez droit sur **Search Server**, puis sur **Index Now**.

   Lors d'une opération de mise à jour, Search Server ne remanie pas l'indice de fond en comble. Il n'indexe que les nouvelles données sur DeviceLock Enterprise Server afin d'ajouter les nouvelles entrées d'indice à l'indice existant.

Tâche: Surveiller et mettre à jour le statut de l'activité d'indexation en cours

Les opérations d'indexation systématique du texte peuvent s'avérer gourmandes en temps et en ressources. Search Server permet de surveiller l'avancement des opérations d'indexation en cours d'exécution.

Le processus d'indexation a lieu en deux étapes. Lors de la première étape, Search Server extrait les principaux mots des copies de réplication et des enregistrements de journaux, puis les enregistre dans des indices temporaires pour chacun des DeviceLock Enterprise Servers indiqués. Pour chaque indice temporaire, Search Server traite 1000 enregistrements par journal.

Lors de la deuxième étape, autrement dit une fois le nombre d'indices temporaires supérieur ou égal à 50, ou au bout de 10 minutes, tous les indices temporaires sont combinés sous forme d'indice principal permanent utilisé pour les recherches. Ce processus de consolidation des indices temporaires sous forme d'indice principal reçoit le nom de fusion.

Search Server comporte des indicateurs d'indexation ainsi que d'avancement et de statut du processus de fusion.

Indicateurs d'avancement et de statut d'indexation

Il est possible de vérifier le processus d'indexation sur chacun des DeviceLock Enterprise Servers indiqués en en examinant le statut et le degré d'avancement. L'indicateur de statut reflète le statut de l'opération d'indexation. Le tableau suivant contient les différents statuts possibles et leurs descriptions.

STATUT	DESCRIPTION
Idle	L'indexation n'a pas encore eu lieu
Waiting	En attente du démarrage de l'indexation
Indexing <*nom_de_journal*>	Indexation en cours

Le compteur d'avancement indique le pourcentage du processus d'indexation déjà effectué.

Indicateurs d'avancement et de statut du processus de fusion

Il est possible de contrôler le processus de fusion en examinant son statut et son degré d'avancement. L'indicateur de statut reflète le statut de l'opération de fusion. Le tableau suivant contient les différents statuts possibles et leurs descriptions.

STATUT	DESCRIPTION
Idle	La fusion n'a pas encore eu lieu
Merging	La fusion est en cours

STATUT	DESCRIPTION
Defragmenting	Compression (optimisation) de l'indice. La compression de l'indice permet d'optimiser la structure de l'indice, en supprimant les données obsolètes et en défragmentant les structures de recherche pour de meilleures performances.

Le compteur d'avancement indique le pourcentage du processus de fusion déjà effectué.

Pour surveiller et mettre à jour le statut de l'activité d'indexation en cours

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Search Server**.
2. Dans **Search Server**, sélectionnez **Current Activity**.

   Lorsque vous sélectionnez Current Activity dans l'arborescence de console, les indicateurs d'avancement et de statut d'indexation et de fusion s'affichent dans le panneau d'affichage détaillé.

   Etant donné que le statut des opérations d'indexation et de fusion en cours n'est pas mis à jour automatiquement, il faut effectuer une mise à jour.

   Pour effectuer une mise à jour, choisissez une des procédures suivantes:

   - Dans l'arborescence de console, cliquez droit sur **Current Activity**, puis sur **Refresh**.
     - OU -
   - Dans l'arborescence de console, sélectionnez **Current Activity**, puis cliquez sur l'option **Refresh** de la barre d'outils.
     - OU -
   - Dans l'arborescence de console, sélectionnez **Current Activity**. Dans la colonne **Name** du panneau d'affichage détaillé, cliquez droit sur n'importe quel nom de DeviceLock Enterprise Server ou sur **Merge Index**, puis cliquez sur **Refresh**.
     - OU -
   - Dans l'arborescence de console, sélectionnez **Current Activity**. Dans le panneau d'affichage détaillé, sélectionnez le nom de n'importe quel DeviceLock Enterprise Server ou **Merge Index**, puis cliquez sur l'option **Refresh** de la barre d'outils.

Utilisation de Search Server

L'utilisation de Search Server comprend les tâches suivantes:

- Recherche systématique de texte
- Utilisation des résultats de recherche

Effectuer une recherche systématique de texte

Search Server permet d'identifier toutes les occurrences d'un mot ou d'une phrase dans la base de données DeviceLock Enterprise Server. Etant donné que la plupart des recherches renvoient un grand nombre de résultats, il est possible de définir des options de recherche afin de limiter et d'optimiser la recherche. Les options de recherche indiquent la manière

dont les résultats de recherche doivent être renvoyés. Les options de recherche permettent de préciser

- Le nombre de résultats de recherche à renvoyer par page.
- Le mode de filtrage des résultats de recherche obtenus. Les résultats de recherche peuvent être filtrés par date et par journal. Par exemple, il est possible de restreindre le nombre de résultats à ceux compris dans une certaine plage de dates et à ceux qui proviennent de certains journaux particuliers.

Voici un certain nombre de points à prendre en compte lors des recherches systématiques de texte:

- Les recherches ne dépendent pas de la case.
- Il est possible de rechercher des mots et des phrases, et d'utiliser des jokers habituels comme les astérisques (*) et les points d'interrogation (?) dans les questions. L'astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser ces caractères génériques n'importe où et en nombre illimité. Pour rechercher une phrase donnée, mettez-la entre guillemets. Pour rechercher plusieurs mots, séparez-les par des espaces.
  Le tableau suivant contient les éléments de recherche, des exemples, et des résultats pour ces types de recherches.

ELEMENT DE RECHERCHE	EXEMPLE	RESULTATS
Mot simple	tarif	Résultats contenant le mot ***tarif***. Ainsi que toutes les variations grammaticales du mot, comme ***tarifs***, ***tarifé*** etc.
Phrase	information confidentielle	Résultats contenant à la fois les mots ***confidentiel*** et ***information***, plutôt que la phrase exacte.
	«information confidentielle»	Résultats contenant la phrase exacte ***information confidentielle***.
Joker	te?te	Résultats contenant ***tente***, ***texte***, etc.
Joker	mon*	Résultats contenant ***mont***, ***monde***, etc.
Joker	*aire	Résultats qui contiennent ***faire***, ***impaire***, ***affaire***, etc.
Joker	actifs *	Résultats contenant ***actifs monétaires***, ***actifs financiers***, ***actifs immobilisés***, ***actifs circulants***, etc.

Pour effectuer une recherche

1. Dans l'arborescence de console, développez **DeviceLock Content Security Server**, puis **Search Server**.

2. Dans **Search Server**, sélectionnez **Search Page**.

   La page de recherche s'affiche dans le panneau d'affichage détaillé.

3. Dans le champ **Search** de la page de recherche, saisissez le mot ou la phrase à trouver. Pour définir des options de recherche, cliquez sur **Options** puis procédez comme suit:

   - Pour préciser le nombre de résultats de recherche à afficher par page, dans la liste **Display…results per page**, cliquez sur l'une ou l'autre des options suivantes: **10**, **20**, **30**, **50**, **100**. Par défaut, le nombre de résultats renvoyé est de 20.
   - Pour limiter le périmètre de recherche à des magasins de données spécifiques, cochez les cases appropriées dans **Limit results to the following logs**.

     Par défaut, Search Server tire les résultats de recherche du journal d'audit, du journal de réplication et du journal des données de réplication supprimées.
   - Pour filtrer les résultats de recherche par date, précisez une plage de dates permettant de limiter les données récupérées. Pour ce faire, définissez les paramètres de dates suivants:

PARAMETRE	DESCRIPTION
From	Indique la date de début de la recherche. Valeurs possibles: **First Record** ou **Records On**. Par défaut, la valeur est **First Record**. En mode **First Record**, Search Server récupère les données en commençant par le premier enregistrement effectué dans le journal. En mode **Records On**, Search Server récupère les données enregistrées à partir d'une date donnée.
To	Indique la date de fin de la recherche. Valeurs possibles: **Last Record** ou **Records On**. Par défaut, la valeur est **Last Record**. En mode **Last Record**, Search Server récupère les données en commençant par le dernier enregistrement effectué dans le journal. En mode **Records On**, Search Server récupère les données enregistrées jusqu'à une date donnée.

     Si vous choisissez le mode **Records On**, cliquez sur les champs **From** et **To** pour afficher le calendrier. Dans le calendrier, cliquez pour sélectionner le jour. Les flèches simples (**<>**) permettent de changer le mois affiché, et les flèches doubles (**<<>>**) de changer l'année affichée.

4. Cliquez sur **Search**.

Utilisation des résultats de recherche

L'utilisation des résultats comprend les tâches suivantes:

- Interprétation des résultats de recherche
- Traitement des résultats de recherche en provenance du journal de réplication

Interprétation des résultats de recherche

Une fois les critères de recherche définis et la recherche lancée, Search Server renvoie une page de résultats de recherche à l'aspect suivant:

customer
Search
Options >>
Results 1 - 3 for customer.
1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View
1

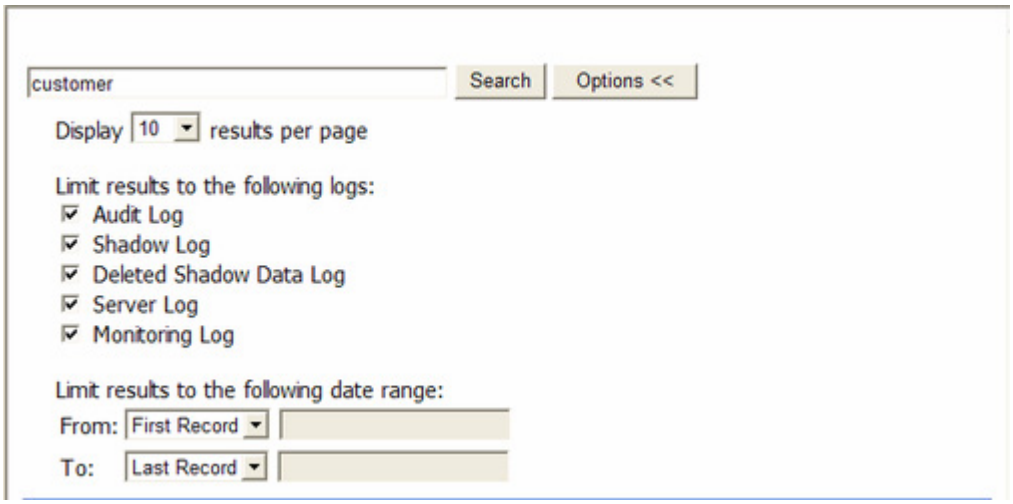
La page des résultats de recherche comporte les domaines d'affichage suivants:

- **Critères de recherche** Affiche les critères de recherche saisis.
- **Barre de statistiques** Indique le nombre de résultats affichés sur la page de résultats de recherche actuelle.
- **Résultats de recherche** Affiche une liste d'éléments numérotés contenant des informations correspondant aux critères de recherche saisis.
- **Navigateur de résultats** Indique le nombre de pages de résultats renvoyées et permet de naviguer d'une page à l'autre.

Chacun de ces domaines fait l'objet d'une description plus détaillée ci-dessous.

Critères de recherche

Ce domaine est situé dans la partie supérieure de chaque page de résultats de recherche. Cliquez sur **Options** pour afficher les critères de recherche supplémentaire indiqués.

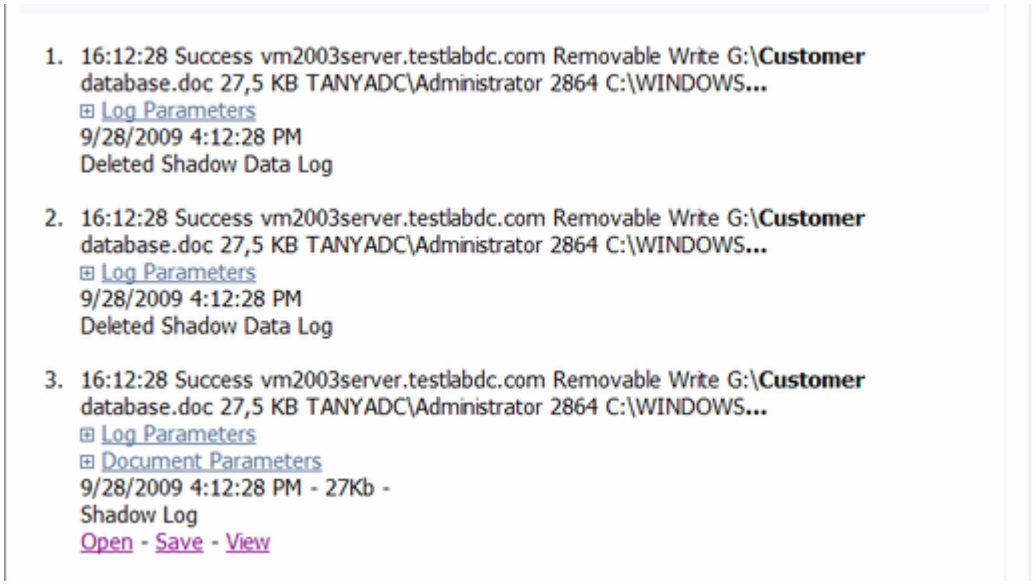


Barre de statistiques

Ce domaine est situé immédiatement au dessus du domaine des résultats de recherche, et a l'aspect suivant.

Résultats de recherche

Ce domaine est situé en dessous du domaine des questions de recherche et de la barre des statistiques, et a l'aspect suivant.


1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View

Chaque résultat de recherche comporte les éléments suivants:

- ***Snippets***: des portions de texte contenant des mots de recherche surlignés (en caractères gras). Ces snippets permettent de voir le contexte dans lequel les mots de

recherche ont été trouvés. La page des résultats de recherche contient uniquement les trois premiers snippets de chaque résultat de recherche.

- ***Log Parameters***: un résumé des informations trouvées dans le journal pour le résultat de recherche considéré. Cliquez sur le signe plus (**+**) pour développer Log Parameters et afficher ces informations. Les informations diffèrent d'un type de journal à l'autre.

  Remarque: Si une entrée de journal est vide, elle n'est pas affichée dans **Log Parameters**.

  Les informations suivantes sont affichées dans **Log Parameters** pour chaque résultat trouvé dans le journal d'audit:

  - **Received Date/Time**: la date et l'heure de réception de l'événement par DeviceLock Enterprise Server.
  - **Type**: la classe d'un événement, à savoir **Success** si l'accès est autorisé ou **Failure** si l'accès est refusé. Cette valeur correspond à celle qui figure dans la colonne **Type** du module d'affichage du journal d'audit du serveur.
  - **Computer**: le nom de l'ordinateur dont provient le journal d'audit. Cette valeur correspond à celle qui figure dans la colonne **Computer** du module d'affichage du journal d'audit du serveur.
  - **Date/Time**: la date et l'heure de réception de l'événement par DeviceLock Service. Cette valeur correspond à celle qui figure dans la colonne **Date/Time** du module d'affichage du journal d'audit du serveur.
  - **Source**: le type de périphérique ou de protocole impliqué. Cette valeur correspond à celle qui figure dans la colonne **Source** du module d'affichage du journal d'audit du serveur.
  - **Action**: le type d'activité de l'utilisateur. Cette valeur correspond à celle qui figure dans la colonne **Action** du module d'affichage du journal d'audit du serveur.
  - **Name**: le nom de l'objet (fichier, clé USB, etc.). Cette valeur correspond à celle qui figure dans la colonne **Name** du module d'affichage du journal d'audit du serveur.
  - **Information**: les autres informations propres au périphérique en rapport avec l'événement, comme les drapeaux d'accès, les noms des périphériques, etc. Cette valeur correspond à celle qui figure dans la colonne **Information** du module d'affichage du journal d'audit du serveur.
  - **User**: le nom de l'utilisateur associé à cet événement. Cette valeur correspond à celle qui figure dans la colonne **User** du module d'affichage du journal d'audit du serveur.
  - **PID**: l'identifiant de la procédure associée à cet événement. Cette valeur correspond à celle qui figure dans la colonne **PID** du module d'affichage du journal d'audit du serveur.
  - **Process**: le chemin d'accès au fichier d'exécution de la procédure. Dans certains cas, le nom de la procédure peut-être affiché en lieu et place du chemin d'accès. Cette valeur correspond à celle qui figure dans la colonne **Process** du module d'affichage du journal d'audit du serveur.
  - **Event**: le numéro qui identifie le type d'événement considéré. Cette valeur correspond à celle qui figure dans la colonne **Event** du module d'affichage du journal d'audit du serveur.

Les informations suivantes sont affichées dans **Log Parameters** pour chaque résultat trouvé dans le journal d'audit ou le journal des données de réplication supprimées:

- **Received Date/Time**: la date et l'heure de réception des données par DeviceLock Enterprise Server.
- **Status**: indique le statut de l'élément. Le statut **Success** (succès) indique que la donnée est bien enregistrée; le statut **Incomplete** (incomplet) indique que la donnée n'est probablement pas complètement enregistrée, alors que le statut **Failed** (échec) est attribué aux réplications de fichiers dont la transmission a été bloquée par les règles contextuelles.
- **Computer**: le nom de l'ordinateur dont provient le journal de réplication. Cette valeur correspond à celle qui figure dans la colonne **Computer** du module d'affichage du journal de réplication du serveur.
- **Date/Time**: la date et l'heure du transfert de données. Cette valeur correspond à celle qui figure dans la colonne **Date/Time** du module d'affichage du journal de réplication du serveur.
- **Source**: le type de périphérique ou de protocole impliqué. Cette valeur correspond à celle qui figure dans la colonne **Source** du module d'affichage du journal de réplication du serveur.
- **Action**: le type d'activité de l'utilisateur. Cette valeur correspond à celle qui figure dans la colonne **Action** du module d'affichage du journal de réplication du serveur.
- **File Name**: le chemin d'accès initial au fichier, ou le nom généré automatiquement si les données n'étaient pas à l'origine un fichier (par exemple des images de CD/DVD, des données écrites directement sur le média ou transférées par les ports parallèle/série). Cette valeur correspond à celle qui figure dans la colonne **File Name** du module d'affichage du journal de réplication du serveur.
- **File Size**: la taille des données. Cette valeur correspond à celle qui figure dans la colonne **File Size** du module d'affichage du journal de réplication du serveur.
- **User**: le nom de l'utilisateur qui a transféré les données. Cette valeur correspond à celle qui figure dans la colonne **User** du module d'affichage du journal de réplication du serveur.
- **PID**: l'identifiant du processus utilisé pour le transfert de données. Cette valeur correspond à celle qui figure dans la colonne **PID** du module d'affichage du journal de réplication du serveur.
- **Process**: le chemin d'accès au fichier d'exécution de la procédure. Dans certains cas, le nom de la procédure peut-être affiché en lieu et place du chemin d'accès. Cette valeur correspond à celle qui figure dans la colonne **Process** du module d'affichage du journal de réplication du serveur.

Les informations suivantes sont affichées dans **Log Parameters** pour chaque résultat trouvé dans le journal de serveur:

- **Type**: la classe de l'événement, soit **Success**, **Information**, **Warning** ou **Error**. Cette valeur correspond à celle qui figure dans la colonne **Type** du module d'affichage du journal du serveur.
- **Date/Time**: la date et l'heure de l'événement. Cette valeur correspond à celle qui figure dans la colonne **Date/Time** du module d'affichage du journal du serveur.

- **Event**: le numéro qui identifie le type d'événement considéré. Cette valeur correspond à celle qui figure dans la colonne **Event** du module d'affichage du journal du serveur.
- **Information**: des informations propres à l'événement, comme des descriptions d'erreurs ou d'avertissements, les noms et valeurs des paramètres modifiés, etc. Cette valeur correspond à celle qui figure dans la colonne **Information** du module d'affichage du journal du serveur.
- **Server**: le nom du serveur sur lequel s'est produit l'événement. Cette valeur correspond à celle qui figure dans la colonne **Server** du module d'affichage du journal du serveur.
- **Record N**: le numéro de l'enregistrement. Cette valeur correspond à celle qui figure dans la colonne **Record N** du module d'affichage du journal du serveur.

Les informations suivantes sont affichées dans **Log Parameters** pour chaque résultat trouvé dans le journal de surveillance:

- **Type**: la classe de l'événement, soit **Success**, **Information**, **Warning** ou **Error**. Cette valeur correspond à celle qui figure dans la colonne **Type** du module d'affichage du journal de surveillance du serveur.
- **Date/Time**: la date et l'heure de l'événement. Cette valeur correspond à celle qui figure dans la colonne **Date/Time** du module d'affichage du journal de surveillance du serveur.
- **Event**: le numéro qui identifie le type d'événement considéré. Cette valeur correspond à celle qui figure dans la colonne **Event** du module d'affichage du journal de surveillance du serveur.
- **Task Name**: le nom de la tâche responsable de cet événement. Peut être vide si l'événement n'est lié à aucune tâche. Cette valeur correspond à celle qui figure dans la colonne **Task Name** du module d'affichage du journal de surveillance du serveur.
- **Computer Name**: le nom de l'ordinateur appartenant à la tâche qui est responsable de cet événement. Peut être vide si l'événement ne concerne pas l'ordinateur considéré. Cette valeur correspond à celle qui figure dans la colonne **Computer Name** du module d'affichage du journal de surveillance du serveur.
- **Information**: information liée à l'événement, comme le statut, une erreur, un avertissement, etc. Cette valeur correspond à celle qui figure dans la colonne **Information** du module d'affichage du journal de surveillance du serveur.
- **Server**: le nom du serveur sur lequel s'est produit l'événement. Cette valeur correspond à celle qui figure dans la colonne **Server** du module d'affichage du journal de surveillance du serveur.
- **Record N**: le numéro de l'enregistrement. Cette valeur correspond à celle qui figure dans la colonne **Record N** du module d'affichage du journal de surveillance du serveur.

- ***Document Properties***: un résumé des informations trouvées dans les propriétés du document pour le résultat de recherche considéré. Ces informations sont récupérées au hazard et affichées uniquement pour les copies de réplication. Cliquez sur le signe plus (**+**) pour développer **Document Properties** et afficher ces informations. Les informations diffèrent d'un type de fichier à l'autre. Par exemple, les informations

suivantes sont affichées dans **Document Properties** pour une copie de réplication de document Word:

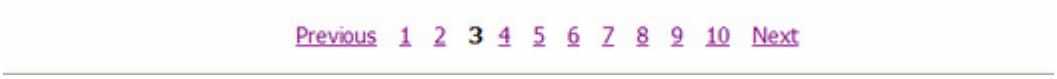
- **Application:** Microsoft Office Word.
- **Author:** le nom de l'utilisateur ayant créé le document.
- **Created:** la date et l'heure de création du document.
- **LastSaved:** la date et l'heure de dernier enregistrement du document.
- **LastSavedBy:** le nom du dernier utilisateur ayant enregistré le document.
- **RevisionNumber:** le nombre d'enregistrements du document.
- **Template:** le nom du modèle associé au document.
- **Title:** le nom du document.
- **TotalEditingTime:** le nombre de minutes pendant lesquelles le document a été ouvert pour y effectuer des changements depuis sa création.

- ***La date et l'heure de création de l'entrée de journal.***
- ***La taille de l'entrée de journal.*** Cette valeur est affichée uniquement pour les copies de réplication obtenues à partir du journal de réplication.
- ***Le nom du journal contenant des résultats de recherche***.
- ***Open, Save and View links***: permet d'accéder et de traiter les résultats de recherche (copies de réplication) en provenance du journal de réplication. Pour en savoir plus sur le mode de traitement des copies de réplication, reportez-vous au chapitre «Traitement des résultats de recherche en provenance du journal de réplication.»

Remarque: Si votre recherche n'a pas produit de résultats, la page de résultats de recherche affiche un message pour l'indiquer.

Navigateur de résultats

Ce domaine est situé dans la partie inférieure de la page des résultats de recherche et a l'aspect suivant.



Pour passez d'un résultat à l'autre, cliquez sur **Next** ou **Previous** ou sur le numéro de page.

Traitement des résultats de recherche en provenance du journal de réplication

Les résultats en provenance du journal de réplication peuvent être soumis aux opérations suivantes:

- Ouverture d'une copie de réplication d'un fichier dans son application d'origine.
- Enregistrement d'une copie de réplication d'un fichier dans n'importe quel emplacement local ou de réseau.

- Ouverture et enregistrement d’une copie de réplication d’un fichier à l’aide du module d’affichage intégré.

On trouvera ci-dessous des instructions détaillées sur la façon d’effectuer ces opérations.

Ouverture d’une copie de réplication d’un fichier dans son application d’origine

1. Effectuez votre recherche.
2. Sur la page des résultats de recherche, cliquez sur le bouton **Open** situé sous le résultat de recherche souhaité.

   La copie de réplication du fichier s’ouvre dans son application d’origine.

   En l’absence d’application d’origine, la boîte de dialogue Open With apparaît. Utilisez cette boîte de dialogue pour choisir le programme devant servir à ouvrir le fichier.

   Si vous ouvrez une copie de réplication d’un fichier saisi à partir soit d’une imprimante, soit d’un périphérique à port parallèle, celle-ci s’ouvre toujours dans le DeviceLock Printer Viewer intégré.

   DeviceLock Printer Viewer permet d'afficher le document imprimé répliqué au format natif du spooler d'imprimante, de le renvoyer à l'imprimante, ou de l'enregistrer sous forme de fichier graphique (de type BMP, GIF, JPEG, PNG, EMF ou TIFF). Les formats de spooler d'imprimante suivants sont pris en charge : PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, impression GDI (ZjStream) et fichiers spoolés EMF.

Enregistrement d’une copie de réplication d’un fichier dans n’importe quel emplacement local ou de réseau

1. Effectuez votre recherche.
2. Sur la page des résultats de recherche, cliquez sur le bouton **Save** situé sous le résultat de recherche souhaité.

   La boîte de dialogue Save As apparaît.

3. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier de réplication.
4. Dans le champ **File name**, saisissez le nom de fichier souhaité.
5. Cliquez sur **Save**.

   Si l'utilisateur a transféré les données sous forme de fichier, elles sont stockées dans le journal de réplication en tant que fichier et peuvent être enregistrées sur l'ordinateur local sous cette forme.

   Lorsque c'est vers un CD/DVD que l'utilisateur a transféré des données, celles-ci sont stockées dans le journal de réplication sous forme d'une image CD/DVD unique (une image par CD/DVD inscrit ou par session), au format CUE.

   Les images CD/DVD, ainsi que les autres données non transférées sous forme de fichier (accès direct au média ou transfert par port parallèle ou série) reçoivent des noms générés automatiquement d'après le type d'action, la lettre du lecteur ou le nom du périphérique et l’heure et la date (par exemple, direct_write(E :). 19:18:29 17.07.2006.bin).

   Les images de CD/DVD sont enregistrées sur l'ordinateur local dans deux fichiers : le fichier de données, dont l'extension est .bin (ex. direct_write(E_) 19_18_29

17_07_2006.bin) et le fichier d'informations (cue sheet) qui a le même nom que le fichier de données associé, avec l'extension .cue (ex. direct_write(E_) 19_18_29 17_07_2006_bin.cue). Les deux fichiers sont nécessaires pour ouvrir l'image CD/DVD dans un logiciel externe qui accepte le format CUE (tel que Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO et autres).

Ouverture et enregistrement d'une copie de réplication d'un fichier à l'aide du module d'affichage intégré

1. Effectuez votre recherche.
2. Sur la page des résultats de recherche, cliquez sur le bouton **View** situé sous le résultat de recherche souhaité.

   La copie de réplication s'ouvre dans le module d'affichage intégré.

3. Dans le module d'affichage intégré, cliquez sur l'une ou l'autre des options d'affichage suivantes:
   - **Hex** affiche les données sous forme hexadécimale et aussi de mots.
   - **Autodetect Text** Permet la détection automatique du codage de texte et affiche les données au format texte uniquement.
   - **ANSI Text** Indique le codage ANSI du texte et affiche les données au format texte uniquement.
   - **UTF-16 Text** Indique le codage UTF-16 du texte et affiche les données au format texte uniquement.
   - **UTF-16BE Text** Indique le codage Unicode UTF-16 (Big Endian) du texte et affiche les données au format texte uniquement.

   Pour enregistrer le fichier, cliquez sur **Save** pour ouvrir la boîte de dialogue **Save As**. Dans la boîte de dialogue **Save As**, procédez comme suit:
   - Dans le champ **Save in**, naviguez jusqu'à l'emplacement dans lequel vous souhaitez enregistrer le fichier.
   - Dans le champ **File name**, saisissez le nom de fichier souhaité.
   - Cliquez sur **Save**.
4. Cliquez sur **Close** pour refermer le module d'affichage.

DeviceLock Group Policy Manager

Présentation

Outre l'administration normale des autorisations assurée par DeviceLock Management Console, DeviceLock propose un mécanisme complémentaire très puissant, qui permet de modifier et de déployer des paramètres via les politiques de groupe dans un domaine Active Directory. Les administrateurs systèmes peuvent utiliser des politiques pour contrôler les paramètres de DeviceLock à partir d'un seul emplacement sur le réseau, quelle que soit sa taille.

Une politique de groupe permet une administration cohérente à l'aide d'Active Directory. Elle utilise les services de répertoire et l'appartenance à un groupe de sécurité pour fournir plus de flexibilité et une meilleure prise en charge des informations de configuration. La politique est configurée à l'aide de la Microsoft Management Console (MMC), la console intégrée d'administration de Microsoft.

DeviceLock permet également une meilleure intégration dans Active Directory. Pour les administrateurs système, cette fonctionnalité clé facilite grandement la gestion et le déploiement dans le cadre de réseaux conséquents. Grâce à l'intégration dans Active Directory, il n'est plus nécessaire d'installer des applications tierces en cas d'administration centralisée, et lors du déploiement. Avec DeviceLock, plus besoin d'avoir sa propre composante à base de serveurs pour contrôler la totalité du réseau; les fonctions standards fournies par Active Directory suffisent.

Avec une politique de groupe, il est possible:

- D'installer DeviceLock Service sur tous les ordinateurs d'un réseau, même ceux qui ne sont pas actuellement sous tension et les ordinateurs nouveaux qui viennent de se connecter au réseau. Pour plus de détails sur le déploiement de DeviceLock Service, veuillez vous reporter au chapitre Installation via Group Policy de ce manuel.
- De contrôler et configurer DeviceLock Service sur un grand nombre d'ordinateurs dans des domaines ou des unités d'organisation différentes simultanément. Même si certains ordinateurs ne sont pas actuellement sous tension ou si ce sont de nouveaux ordinateurs qui se connectent pour la première fois au réseau, ils seront inclus dans le déploiement automatique par DeviceLock des paramètres prédéfinis.
- D'afficher la politique en cours d'application et de prévoir celle qui devrait l'être. Pour plus d'informations, veuillez lire le chapitre Utilisation du RSoP (Resultant Set of Policy) de ce manuel.

Remarque: L'administration de DeviceLock via une politique de groupe nécessite une installation et une configuration correctes d'Active Directory. Pour plus d'informations sur ces pré-requis indispensables, veuillez vous reporter à la documentation de Microsoft.

Appliquer une politique de groupe

La politique s'applique automatiquement au démarrage de l'ordinateur. Lorsqu'un utilisateur allume l'ordinateur, le système applique la politique DeviceLock.

La politique peut éventuellement faire périodiquement l'objet de nouvelles applications. Par défaut, la politique est réappliquée toutes les 90 minutes. Il est toutefois possible de modifier cette fréquence à l'aide du Group Policy Object Editor. Pour en savoir plus, reportez-vous à la base de connaissance Microsoft sur:
http://support.microsoft.com/default.aspx?scid=kb;fr;203607

La politique peut aussi être réappliquée de façon ponctuelle. Pour mettre à jour les paramètres de la politique active sur Windows XP et toute version ultérieure, vous pouvez passer par la ligne de commande de l'utilitaire ***gpupdate.exe /force*** fournie par Microsoft. Sur Windows 2000, merci de vous reporter à la ligne suivante: ***secedit /refreshpolicy machine_policy /enforce***.

Lors du traitement, le système interroge service de répertoire concernant la liste des objets de la politique de groupe (GPO) à appliquer. Chaque GPO est lié à un dossier Active Directory auquel l'ordinateur ou l'utilisateur appartient. Par défaut, le système traite les GPO dans l'ordre suivant: local/ site/domaine/unité organisationnelle. En conséquence, l'ordinateur prend en compte les paramètres de politique du dernier dossier Active Directory traité.

Lors du traitement d'un GPO, le système vérifie la liste des contrôles d'accès (ACL) associés au GPO. Si une entrée du contrôle d'accès (ACE) interdit l'accès de l'ordinateur au GPO, le système n'applique pas les paramètres de politique spécifiés par le GPO. En revanche, si l'ACE autorise l'accès au GPO, alors le système applique les paramètres de politique spécifiés par le GPO.

Règles de transmission de GPO standard

Tous les paramètres non configurés d'un GPO peuvent être ignorés, étant donné qu'ils ne sont pas transmis au reste de l'arborescence ; seuls les paramètres configurés sont transmis. Il y a trois scénarios possibles:

- Le parent a une valeur de paramètre, et l'enfant non.
- Le parent a une valeur de paramètre, et l'enfant a une valeur non conflictuelle pour le paramètre en question.
- Le parent a une valeur de paramètre, et l'enfant a une valeur conflictuelle pour le paramètre en question.

Si un GPO a des paramètres qui sont configurés pour une unité organisationnelle de parent, et que les mêmes paramètres de politique sont non configurés pour une unité organisationnelle enfant, l'enfant hérite les paramètres GPO du parent. Ce qui est logique. Si un GPO a des paramètres configurés pour une unité organisationnelle parent qui ne

rentre pas en conflit avec un GPO sur une unité organisationnelle enfant, l'unité organisationnelle enfant hérite les paramètres GPO du parent et applique également ses propres GPO.

Si un GPO a des paramètres configurés pour une unité organisationnelle parent qui rentre en conflit avec les mêmes paramètres d'un autre GPO configuré pour une unité organisationnelle enfant, l'unité organisationnelle enfant n'hérite pas ce paramètre GPO particulier de l'unité organisationnelle parent. Le paramètre de la politique enfant GPO est prioritaire, même s'il existe un cas dans lequel cela ne se produit pas.

Si le parent désactive un paramètre et que l'enfant modifie ce paramètre, le changement de l'enfant est ignoré. En d'autres termes, la désactivation d'un paramètre est toujours transmise au reste de la hiérarchie.

Démarrage de DeviceLock Group Policy Manager

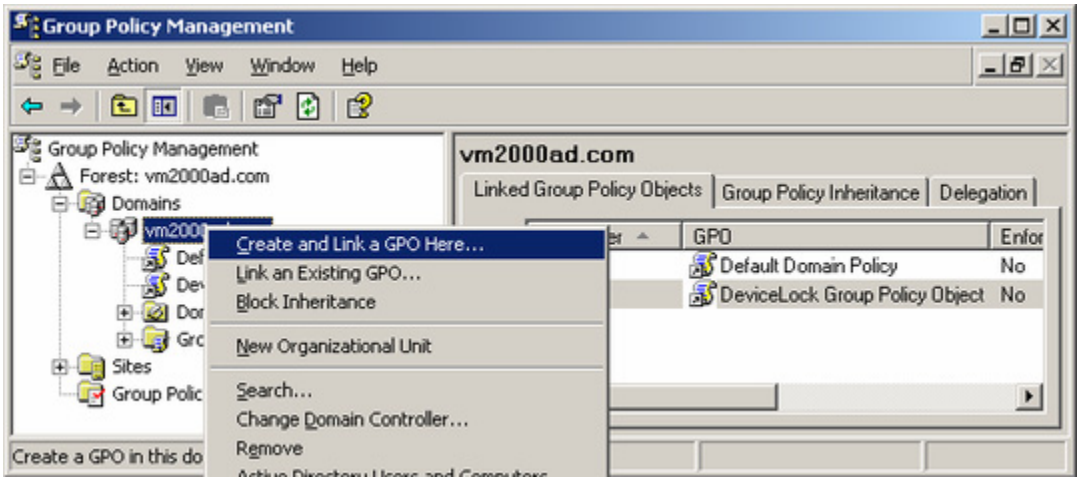
DeviceLock Group Policy Manager s'intègre dans l'éditeur d'objet de politique de groupe (GPO) de Windows. Pour utiliser DeviceLock Group Policy Manager sur votre ordinateur local plutôt que sur le contrôleur de domaine, il faut que l'éditeur GPO soit installé localement. Il est conseillé d'installer la Group Policy Management Console (GPCM). Vous pouvez le télécharger gratuitement à partir du Centre de téléchargements Microsoft.

Pour ouvrir DeviceLock Group Policy Manager, il faut d'abord démarrer l'éditeur GPO.

1. Démarrez le module Group Policy Management intégré.

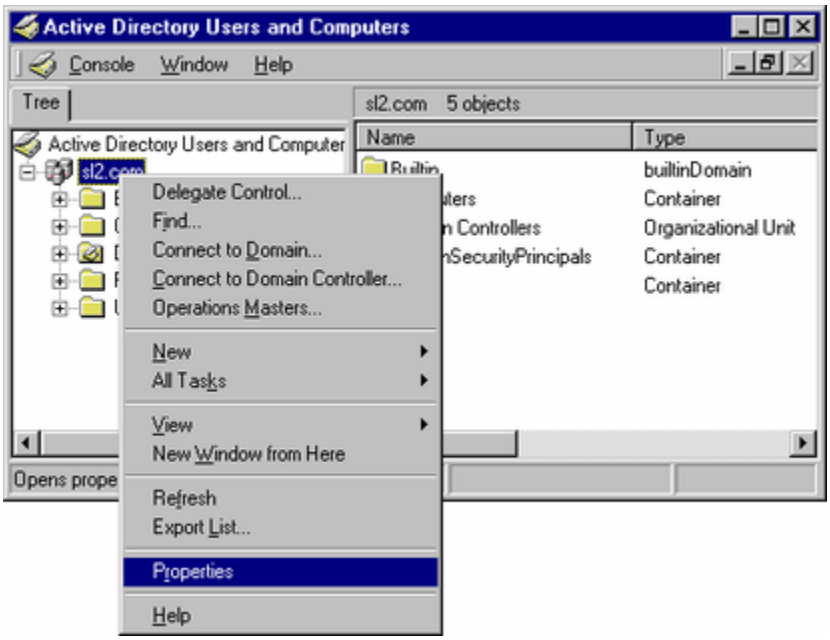
   Si le module Group Policy Management n'est pas installé sur votre ordinateur, vous pouvez le remplacer en utilisant le module Active Directory Users and Computers.

2. Dans l'arborescence de console, sélectionnez votre domaine.

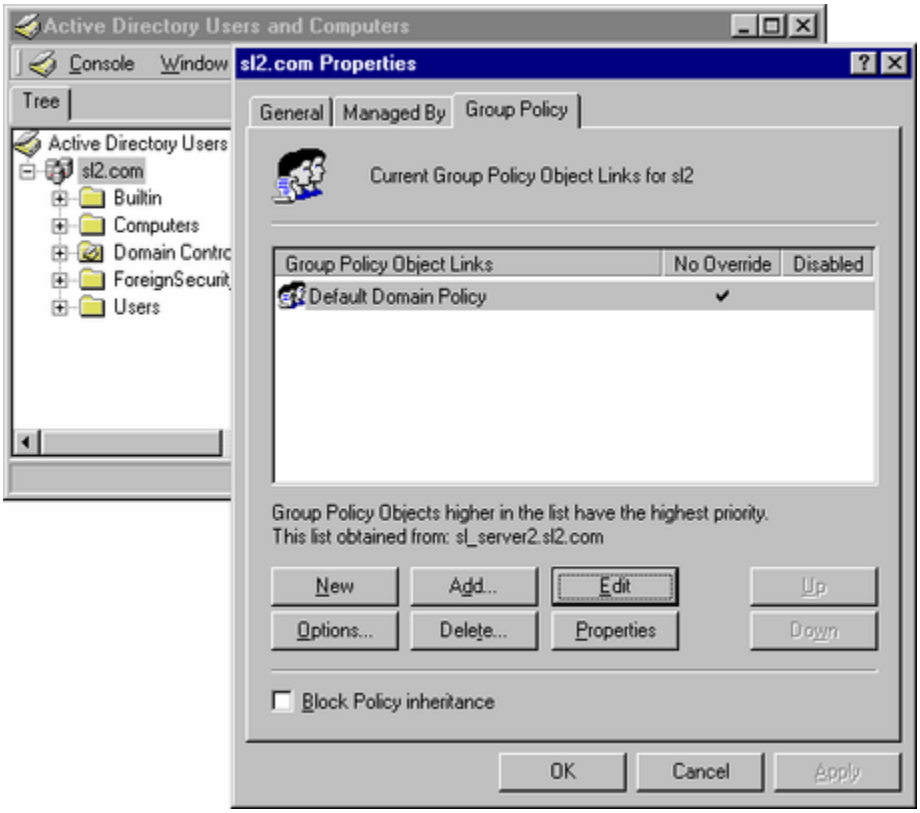


3. Choisissez l'objet de politique de groupe dont vous avez besoin, puis cliquez sur **Edit** dans le menu contextuel accessible par simple clic droit de votre souris. Pour créer un nouvel objet de politique de groupe, cliquez sur **Create and Link a GPO Here** à l'aide du menu contextuel du domaine.

Si vous utilisez le module Active Directory Users and Computers, cliquez droit sur votre domaine, puis cliquez sur **Properties**.

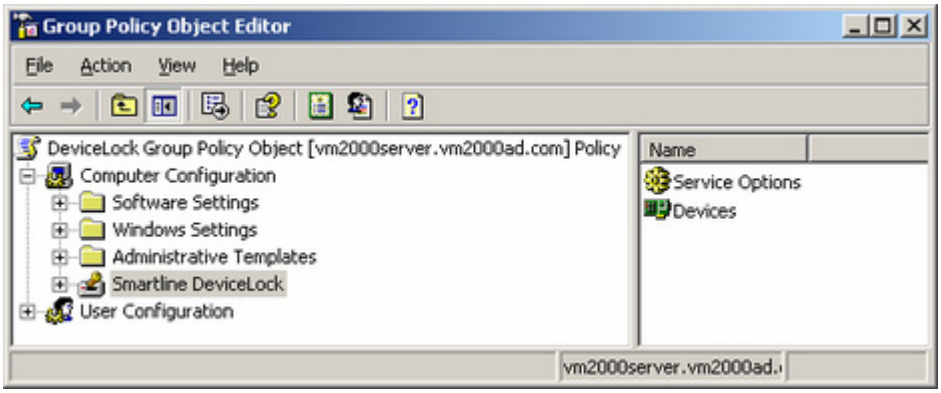


Cliquez sur l'onglet **Group Policy** et choisissez une politique de groupe, puis cliquez sur **Edit**. Pour créer une nouvelle politique de groupe, cliquez sur **Add**.



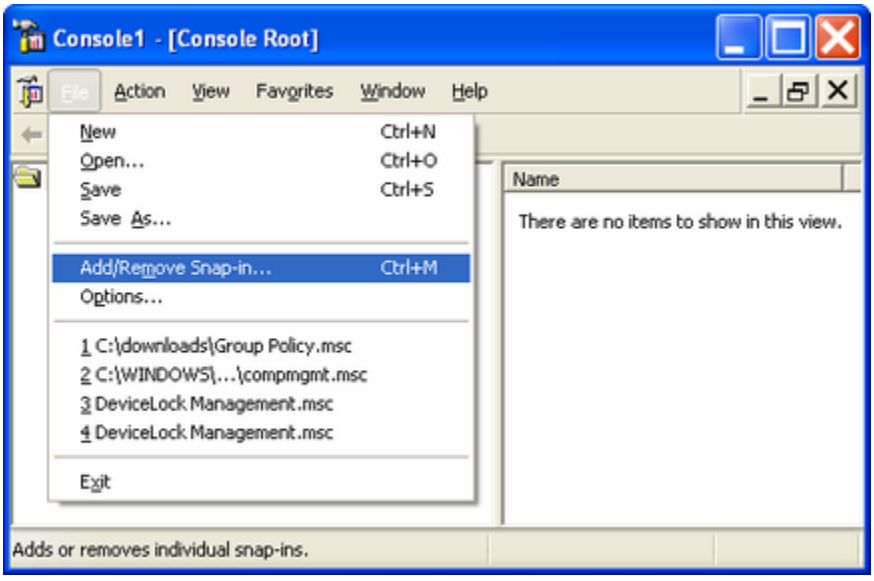
4. Attendez le démarrage de l'éditeur GPO. Ceci peut prendre quelques secondes.

5. Dans **Computer Configuration**, choisissez **DeviceLock**.

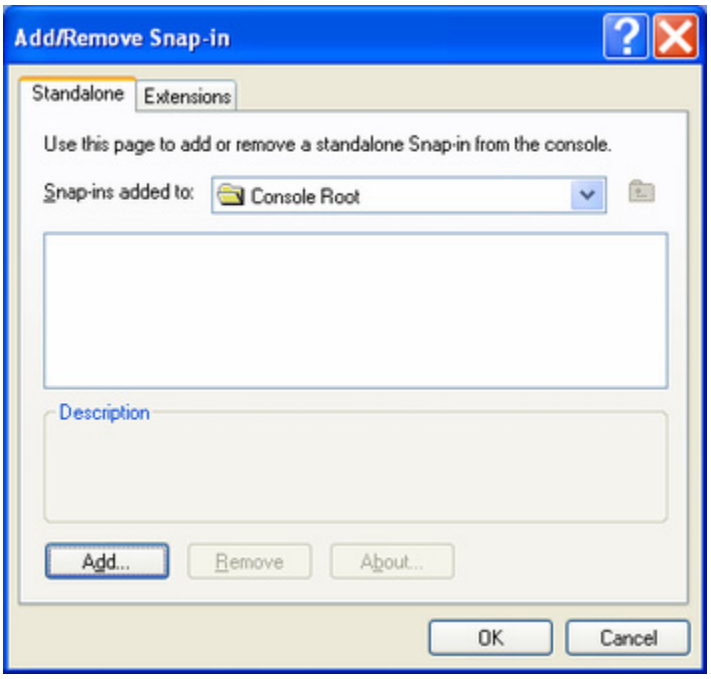


Pour démarrer l'éditeur GPO, il est également possible de démarrer MMC et d'ajouter la politique de groupe intégrée manuellement:

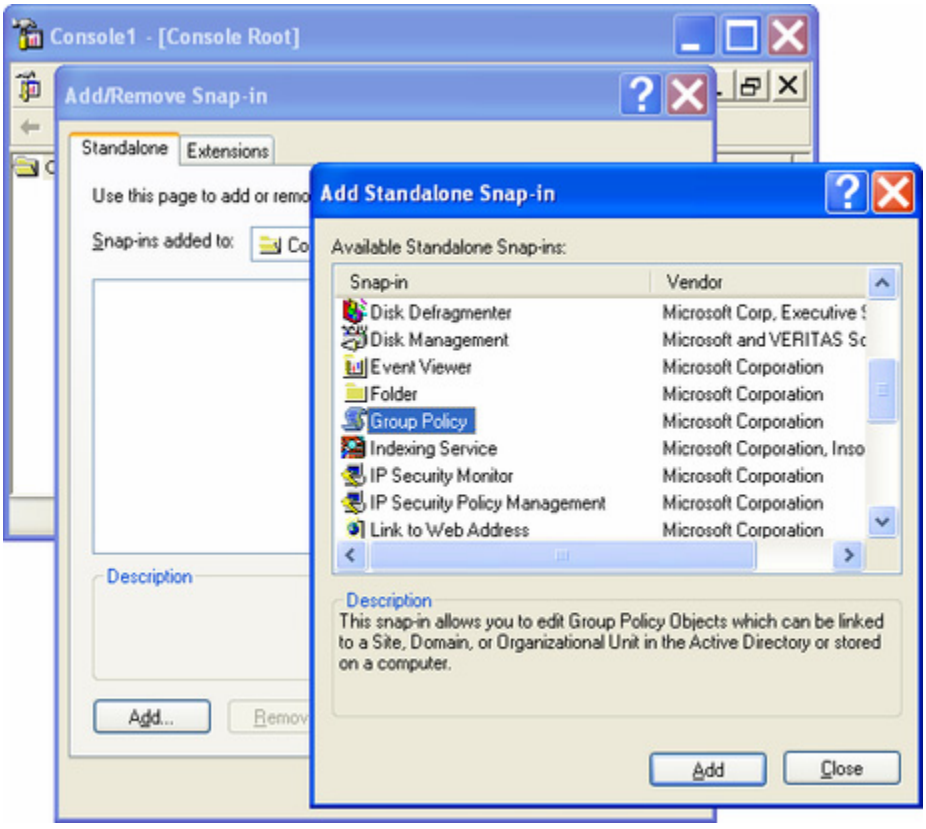
1. Lancez **mmc** à partir de la ligne de commande ou utilisez le menu **Run** pour exécuter cette commande.
2. Ouvrez le menu **File**, puis cliquez sur **Add/Remove snap-in**.



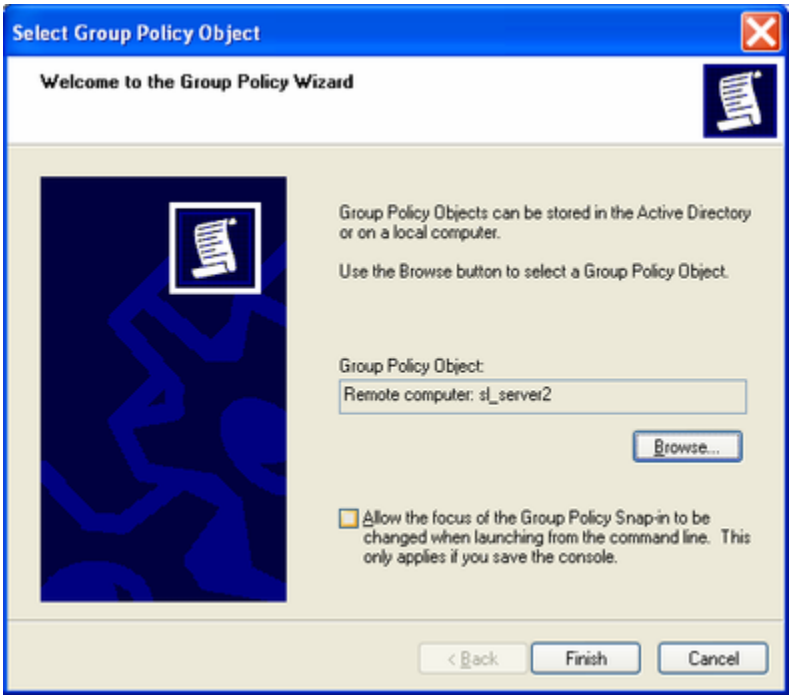
3. Cliquez sur l'onglet **Standalone**, puis sur **Add**.



4. Choisissez **Group Policy** dans la liste, puis cliquez sur **Add**.



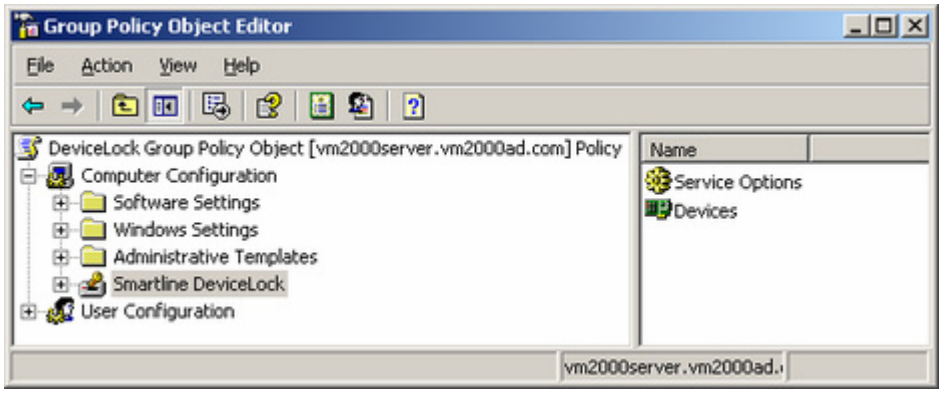
5. Choisissez une politique de groupe, soit dans Active Directory, soit à partir d'un ordinateur local, puis cliquez sur **Finish**.


Select Group Policy Object
Welcome to the Group Policy Wizard
Group Policy Objects can be stored in the Active Directory or on a local computer.
Use the Browse button to select a Group Policy Object.
Group Policy Object:
Remote computer: sl_server2
Browse...
Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel

6. Cliquez sur **Close** pour fermer la fenêtre **Add Standalone Snap-in**.
7. Cliquez sur **OK** pour ajouter le progiciel.
8. Ouvrez le dossier **Computer Configuration**, puis choisissez **DeviceLock**.

Utilisation de DeviceLock Group Policy Manager

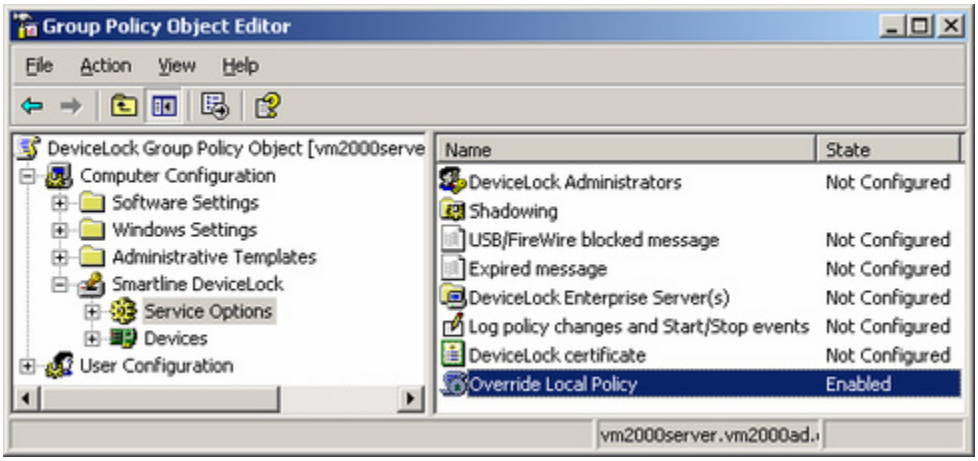
Il n’y a presque aucune différence entre l'administration de DeviceLock Service avec DeviceLock Management Console et avec DeviceLock Group Policy Manager. Pour plus d’informations, veuillez lire le chapitre Administration de DeviceLock Service de ce manuel.



Il est impossible d'administrer DeviceLock Enterprise Server ou de visionner les journaux d’audit et de réplication à l'aide de DeviceLock Group Policy Manager. Pour ce faire, utilisez DeviceLock Management Console.

Par rapport à l'administration avec DeviceLock Management Console, l'administration de DeviceLock Service avec DeviceLock Group Policy Manager apporte quatre fonctionnalités supplémentaires.

1. **Override Local Policy**: si vous voulez empêcher les modifications de paramètres, d'autorisations et de politique d'audit sur les postes de travail individuels (sans l'éditeur GPO), choisissez l'option **Override Local Policy** du menu contextuel **Service Options**. Le mode Group Policy sera ainsi activé pour tous les ordinateurs du GPO, interdisant ainsi l'activation du mode Local Policy sur ces ordinateurs.



Si le paramètre Override Local Policy est activé, il sera impossible de désactiver le paramètre Use Group Policy dans les Service Options de la DeviceLock Management Console et du DeviceLock Enterprise Manager.

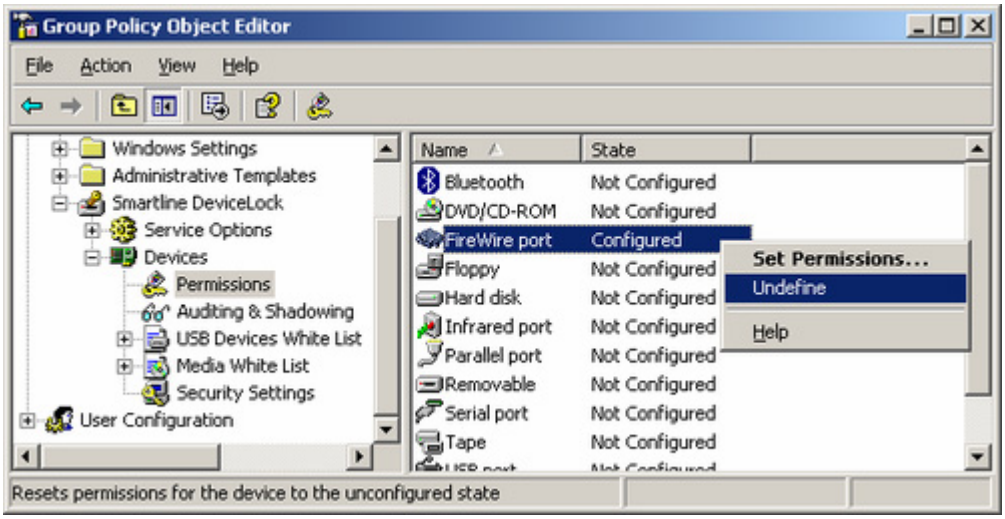
Le tableau suivant montre comment les paramètres **Use Group Policy** et le paramètre **Override Local Policy** affectent le mode de politique des applications:

LE MODE DE POLITIQUE DES APPLICATIONS	USE GROUP POLICY	OVERRIDE LOCAL POLICY
Appliquer seulement la politique locale.	Désactivé	Désactivé
Appliquer seulement la politique de groupe.	Activé	Activé
La politique locale s'applique jusqu'à ce que la réplication Active Directory survienne.	Activé	Désactivé

Lors du réglage du paramètre **Override Local Policy**, prenez en compte ce qui suit:

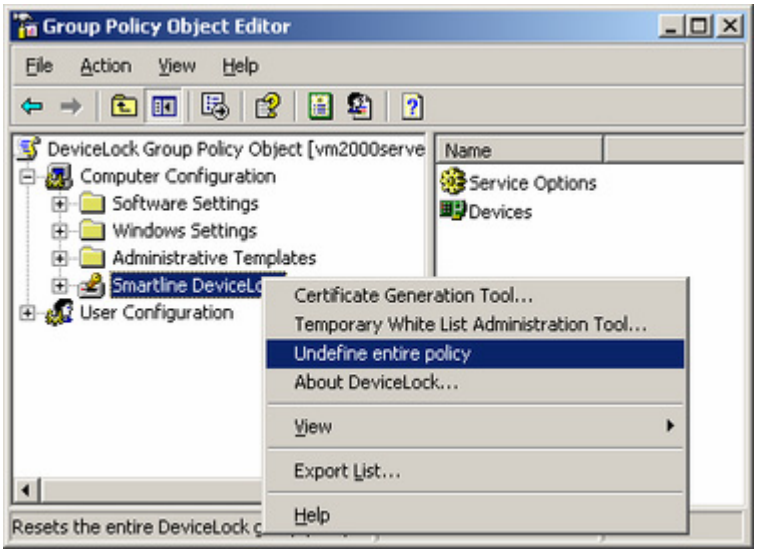
- Désactiver le paramètre **Override Local Policy** n'annule pas la réplication Active Directory.
- Si le paramètre **Override Local Policy** est désactivé, tous les paramètres de DeviceLock Service que vous avez choisis via la console d'administration DeviceLock et DeviceLock Enterprise Manager prennent effet immédiatement.

2. **Undefine**: tout paramètre peut être restauré à l'état non-configuré. Aucun paramètre non-configuré n'est pris en compte dans ce GPO. Pour plus d'informations, veuillez lire le chapitre Règles de transmission de GPO standard de ce manuel.

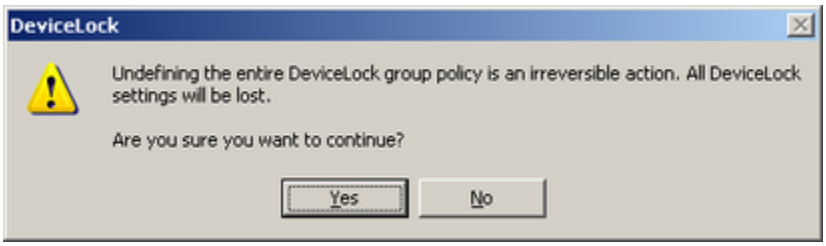


Utilisez l'option **Undefine** du menu contextuel de n'importe quel paramètre pour restaurer l'état initial (non-configuré) de ce paramètre. Certains paramètres peuvent aussi être réinitialisés en grisant la case correspondante.

3. **Undefine entire policy**: vous pouvez restaurer l'état initial de tous les paramètres en un seul clic. Cette option a le même effet que de restaurer chaque paramètre un à un (voir ci-dessus).



Pour restaurer tous les paramètres à l'état initial, choisissez l'option **Undefine entire policy** du menu contextuel de l'élément racine **DeviceLock**.


DeviceLock
Undefining the entire DeviceLock group policy is an irreversible action. All DeviceLock settings will be lost.
Are you sure you want to continue?
Yes
No

4. **Remove Offline**: Vous pouvez supprimer tout paramètre de politique hors ligne (autorisations, règles d'audit et de réplication, listes blanches, etc.) pour les périphériques et pour les protocoles afin que les autorisations habituelles s'appliquent dans ce GPO. Pour ce faire, cliquez droit sur le paramètre de politique concerné, puis cliquez sur **Remove Offline**.

Remarque: Pour gérer les paramètres de DeviceLock via la Politique de groupe, DeviceLock Service doit être installé et démarré sur tous les ordinateurs appartenant au GPO. Pour plus de détails sur l'installation du service, veuillez vous référer au chapitre Déploiement de DeviceLock Service de ce manuel.

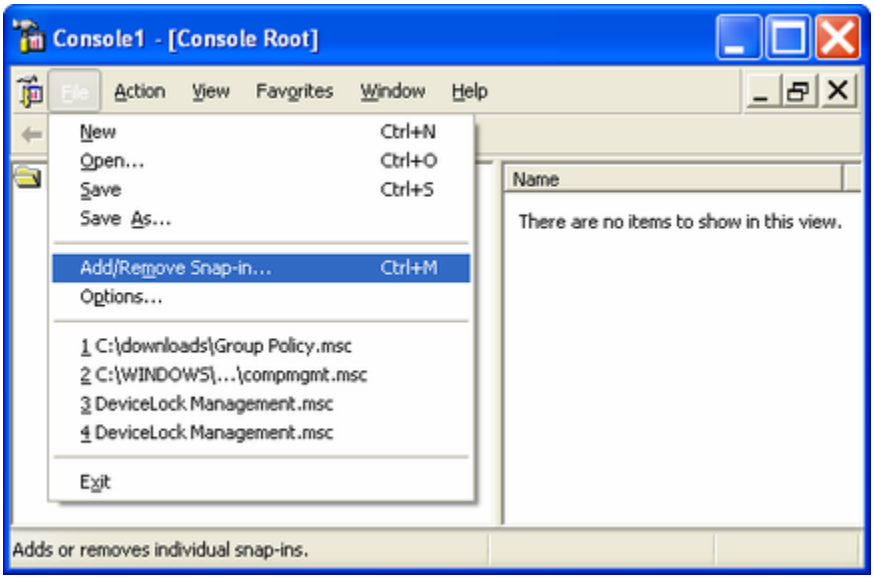
Par ailleurs, gardez à l'esprit le fait que la Politique de groupe étant réappliquée à intervalles réguliers (par défaut, toutes les 90 minutes) vos modifications ne sont pas prises en compte de façon immédiate. Pour plus d'informations, merci de vous reporter au chapitre Appliquer une Politique de groupe de ce document.

Utilisation de RSoP (Resultant Set of Policy)

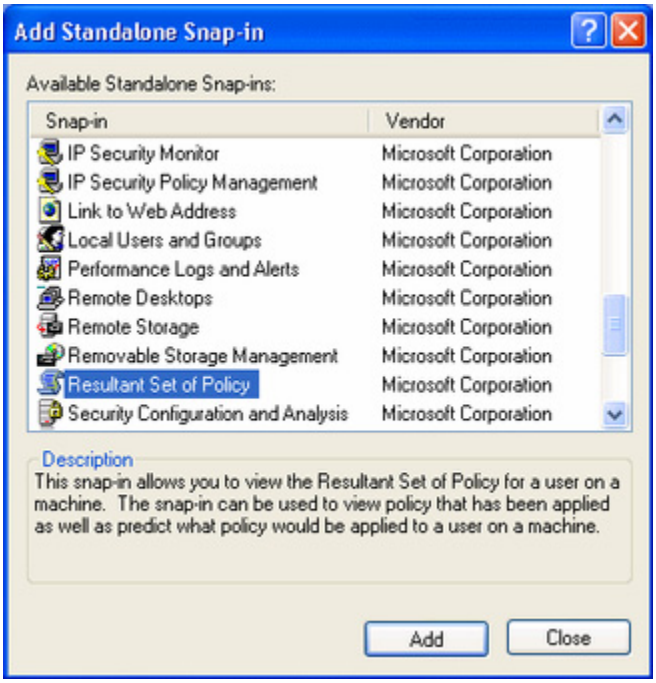
DeviceLock prend en charge le Resultant Set of Policy, si bien que vous pouvez utiliser le snap-in Windows standard pour afficher la politique DeviceLock actuellement appliquée, ainsi que pour prédire la politique susceptible d'être appliquée à un ordinateur donné.

Pour utiliser le RSoP, démarrer MMC et ajoutez manuellement le snap-in Resultant Set of Policy:

1. Lancez **mmc** à partir de la ligne de commande ou utilisez le menu **Run** pour exécuter cette commande.
2. Ouvrez le menu **File**, puis cliquez sur **Add/Remove snap-in**.

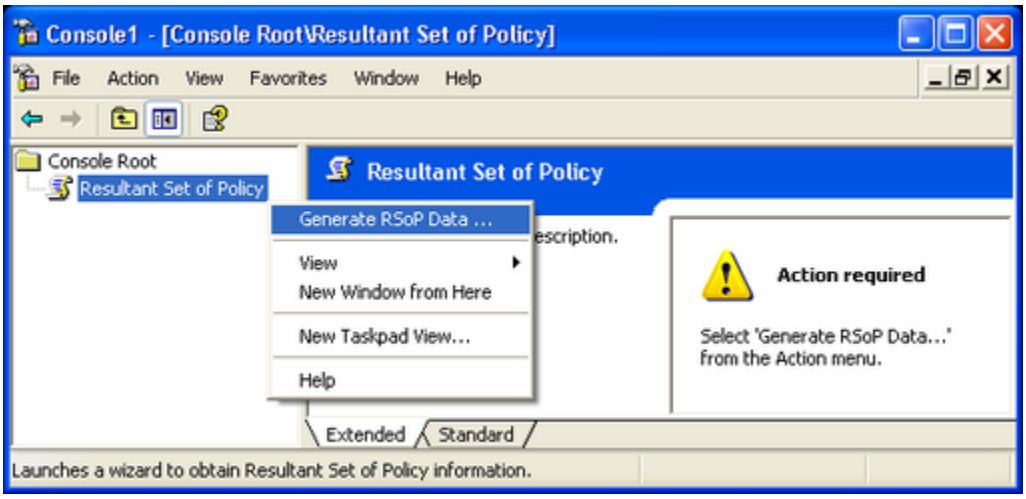


3. Cliquez sur l'onglet **Standalone**, puis sur **Add**.
4. Choisissez **Resultant Set of Policy** dans la liste, puis cliquez sur **Add**.

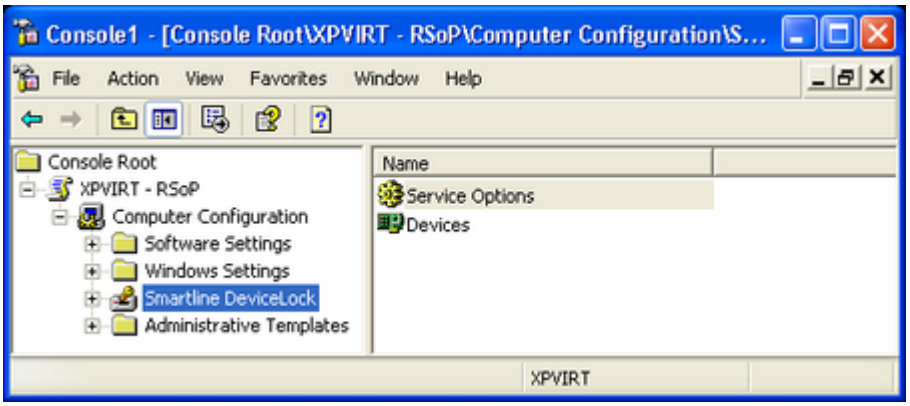

Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Vendor
IP Security Monitor Microsoft Corporation
IP Security Policy Management Microsoft Corporation
Link to Web Address Microsoft Corporation
Local Users and Groups Microsoft Corporation
Performance Logs and Alerts Microsoft Corporation
Remote Desktops Microsoft Corporation
Remote Storage Microsoft Corporation
Removable Storage Management Microsoft Corporation
Resultant Set of Policy Microsoft Corporation
Security Configuration and Analysis Microsoft Corporation
Description
This snap-in allows you to view the Resultant Set of Policy for a user on a machine. The snap-in can be used to view policy that has been applied as well as predict what policy would be applied to a user on a machine.
Add
Close

5. Cliquez sur **Close** pour refermer la fenêtre **Add Standalone Snap-in** puis sur **OK** pour ajouter le snap-in.

6. Sélectionnez **Resultant Set of Policy** dans l'arborescence de console.


Console1 - [Console Root\Resultant Set of Policy]
File Action View Favorites Window Help
Console Root
Resultant Set of Policy
Resultant Set of Policy
Generate RSoP Data ...
View
New Window from Here
New Taskpad View...
Help
Action required
Select 'Generate RSoP Data...' from the Action menu.
Extended Standard
Launches a wizard to obtain Resultant Set of Policy information.

7. Cliquez sur **Generate RSoP Data** dans le menu contextuel accessible à l'aide du bouton droit de la souris.
8. Parcourez l'assistant Resultant Set of Policy Wizard pour obtenir des informations RSoP à partir de l'ordinateur sélectionné.
9. Ouvrez le dossier **Computer Configuration**, puis choisissez **DeviceLock**.



Remarque: RSoP ne permet pas de modifier la politique, car tous les paramètres sont en mode de lecture seule.

RSoP est très utile pour deviner le GPO à appliquer à l'ordinateur.

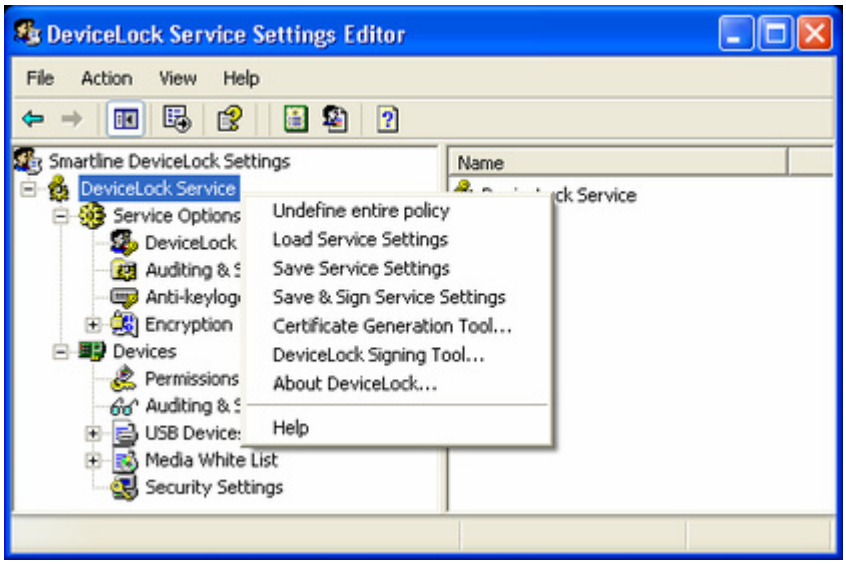
Pour plus d'informations sur Resultant Set of Policy, reportez-vous à l'article en ligne de Microsoft: http://technet.microsoft.com/fr-fr/library/cc775741(WS.10).aspx.

DeviceLock Service Settings Editor

Présentation

DeviceLock Service Settings Editor sert à créer et modifier des fichiers XML avec les paramètres, les autorisations et les régles d'audit et de replication nécessaires pour DeviceLock Service.

DeviceLock Service Settings Editor s'installe en même temps que les autres consoles de gestion.



Il y a peu de différences entre les procédures de définition de politique de DeviceLock Management Console et de DeviceLock Service Settings Editor. Pour plus d'informations, veuillez consulter la section Administration de DeviceLock Service du présent manuel.

En comparaison avec la DeviceLock Management Console de DeviceLock Service Settings Editor:

- Pas besoin de se connecter à un ordinateur avec DeviceLock Service. DeviceLock Service Settings Editor modifie et enregistre les paramètres des fichiers XML externes et permet de créer et éditer les politiques sans être connecté. Son fonctionnement est semblable à celui de DeviceLock Group Policy Manager, mais il utilise des fichiers XML plutôt que des GPO.
- Tous les paramètres (individuellement ou collectivement) peuvent être restaurés Ã l'état non-configuré. Aucun paramètre non-configuré n'est pris en compte lorsque la politique s'applique à DeviceLock Service.
- Vous pouvez supprimer tout paramètre de politique hors ligne (autorisations, règles d'audit et de réplication, listes blanches, etc.) pour les périphériques et pour les protocoles afin que les autorisations habituelles s'appliquent dans ce fichier de politique.

Pour créer une nouvelle politique sans modèle, exécutez DeviceLock Service Settings Editor et appliquez des changements à la politique par défaut (vide).

Pour modifier une politique existante, chargez le fichier XML contenant cette politique sous DeviceLock Service Settings Editor avec l'élément **Load Service Settings** du menu contextuel et procédez aux modifications souhaitées.

Si vous créez une nouvelle politique sans modèle, vous devrez sélectionner **Save Service Settings** dans le menu contextuel afin d'enregistrer la nouvelle politique dans un fichier XML. Vous pouvez aussi utiliser **Save & Sign Service Settings** dans le menu contextuel pour sauvegarder une politique dans un fichier XML externe et le signer automatiquement avec le certificat DeviceLock le plus récent (la clé privée). L'élément de menu **Save & Sign Service Settings** est désactivé lorsqu'aucune clé privée n'est encore chargée dans le DeviceLock Signing Tool.

Par la suite, les fichiers contenant des politiques créées à l'aide de DeviceLock Service Settings Editor peuvent être chargés via DeviceLock Management Console et/ou DeviceLock Group Policy Manager.

Ces fichiers contenant des politiques peuvent aussi être envoyés aux utilisateurs dont les ordinateurs ne sont pas en ligne et par conséquent hors de portée via les consoles de gestion. Pour éviter toute modification non autorisée, les fichiers doivent être signés avec le DeviceLock Certificate (la clé privée) à l'aide du DeviceLock Signing Tool. Pour plus d'informations, veuillez consulter la section Paramètres de service du présent manuel.

Si vous modifiez un fichier de politique existant, DeviceLock Service Settings Editor enregistrement automatiquement vos modifications.

Remarque: Seuls les paramètres explicitement définis dans un fichier de politiques s'appliquent aux postes client. Tous les paramètres ayant le statut **Not Configured** sont ignorés par les ordinateurs client.

DeviceLock Service Settings Editor utilise aussi le plug-in Set Service Settings de DeviceLock Enterprise Manager. Ce plug-in exécute DeviceLock Service Settings Editor en tant qu'application externe et l'ouvre avec le fichier XML sélectionné dans la boîte de dialogue des paramètres du plug-in.

Lorsque vous modifiez une politique (modifications des paramètres, des autorisations, définition de la liste blanche, etc.) dans le fichier XML ouvert par le plug-in avec l'éditeur, DeviceLock Service Settings Editor enregistre les modifications dans ce fichier. Une fois la politique modifiée, fermez DeviceLock Service Settings Editor et retournez dans la boîte de dialogue des paramètres du plug-in.

Pour plus d'informations, veuillez consulter la section Définition des paramètres de service du présent manuel.

DeviceLock Enterprise Manager

Présentation

DeviceLock Enterprise Manager permet de vérifier et de changer les politiques de sécurité définies pour les types de périphériques et les protocoles; d'installer, de mettre à jour et de supprimer DeviceLock Service; et de visionner les journaux d'audit et de réplication pour tous les ordinateurs d'un réseau important. Il est recommandé d'utiliser DeviceLock Enterprise Manager dans les réseaux importants sans Active Directory.

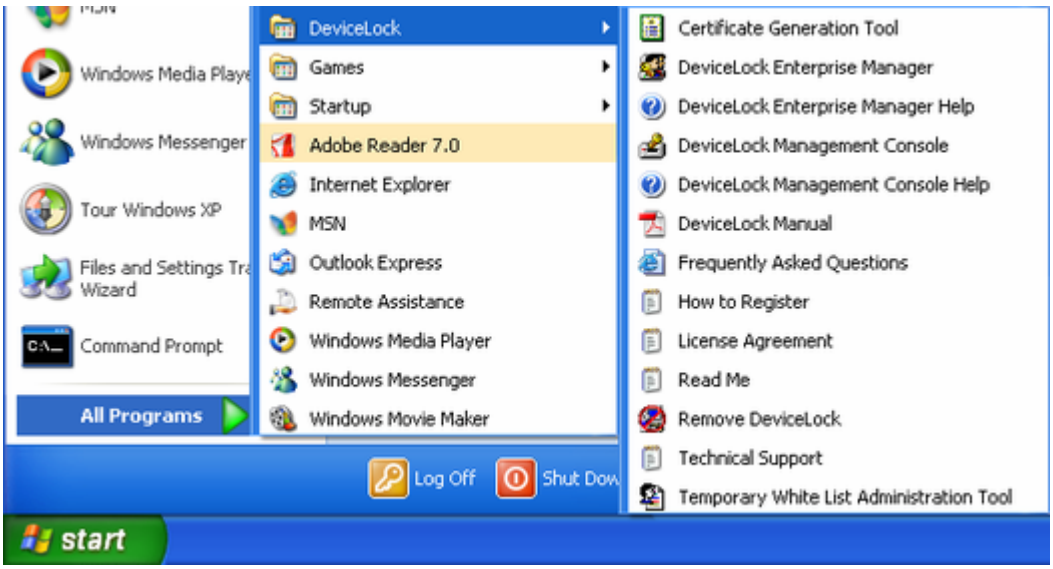
Équipée d'un moteur multitraitement, cette console accélère les procédures pour tous les ordinateurs d'un réseau important.

DeviceLock Enterprise Manager stocke, compare et filtre les données reçues de tous les ordinateurs. Les administrateurs peuvent prendre des «instantanés» des systèmes afin d'effectuer des comparaisons ultérieures, ou de noter les changements.

DeviceLock Enterprise Manager bénéficie d'une architecture flexible de type plug-in qui permet d'ajouter des modules supplémentaires sur demande si nécessaire. Chaque module d'extension (plug-in) remplit une tâche précise et affiche les informations collectées sur sa propre fenêtre.

Pour des informations sur la manière d'installer DeviceLock Enterprise Manager, veuillez lire la section Installation des consoles de gestion de ce manuel.

Pour exécuter DeviceLock Enterprise Manager, sélectionnez le raccourci approprié du menu **All Programs** disponible en cliquant sur le bouton **Start** de Windows.



Interface

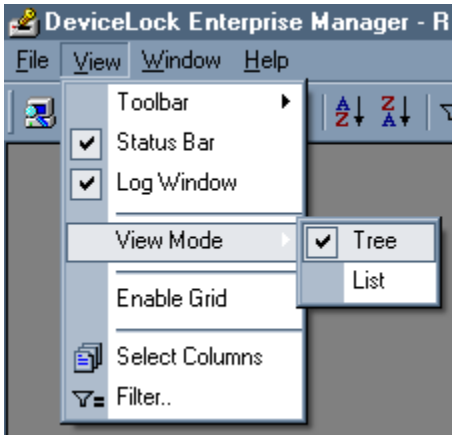
DeviceLock Enterprise Manager possède une structure d'interface multi-documents (MDI) qui permet d'affecter une fenêtre à chaque tâche.

La fenêtre principale de DeviceLock Entreprise Manager peut être redimensionnée. DeviceLock Enterprise Manager garde en mémoire sa taille et sa position sur votre écran et les restaure lorsque vous redémarrez votre ordinateur.

Le menu situé en haut de la fenêtre principale permet d'accéder à de nombreuses fonctions.

Pour modifier les colonnes affichées dans les fenêtres des plug-ins, cliquez sur **Select Columns** dans le menu **View** ou sur l'icône correspondante dans la barre d'outils principale **(MainToolbar**).

Par défaut, DeviceLock Entreprise Manager affiche l'information reçue des plug-ins sous forme d'arborescence. Cependant cette information peut également être affichée sous forme de liste. Pour modifier le mode d'affichage, cliquez sur **View Mode** dans le menu **View** et sélectionnez **Tree** (arbre) ou **List**. Attention, cette sélection doit être effectuée pour chaque plug-in individuellement.



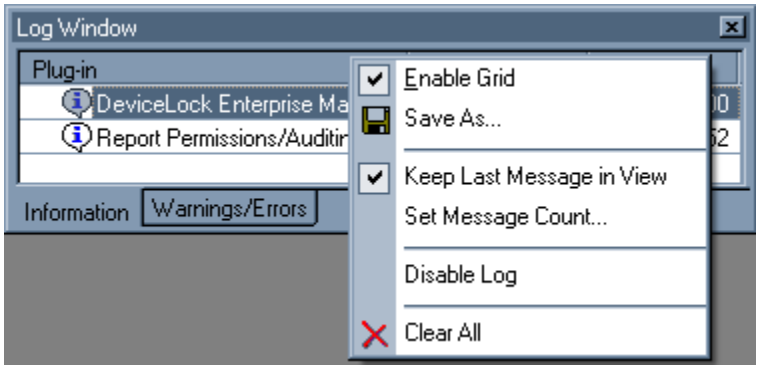
Vous pouvez cacher la barre de statut et/ou la fenêtre de journal en décochant les éléments correspondants dans le menu **View**.

Pour activer les grilles autour des éléments dans la fenêtre des plug-ins, sélectionnez **Enable Grid** dans le menu **View**. Cette sélection est à effectuer pour chaque plug-in séparément.

Pour trier les données dans les fenêtres de plug-in, cliquez sur le titre de la colonne que vous souhaitez trier. Pour revenir sur l'ordre de tri, cliquez à nouveau sur le titre de la colonne.

Si vous avez besoin de trier les éléments situés en haut de l'arbre (comme les domaines et les ordinateurs), utilisez les icônes correspondantes dans la barre d'outils principale (**Main toolbar**).

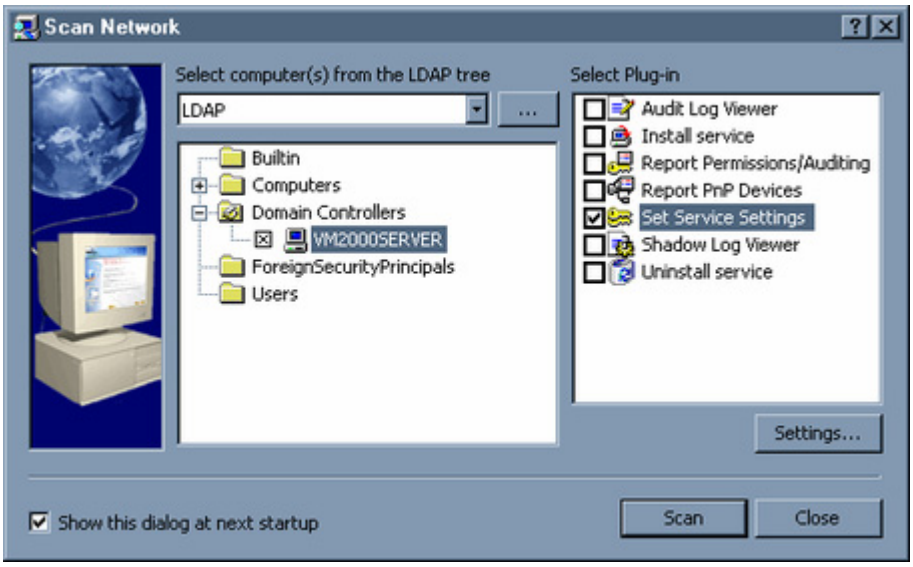
Vous trouverez une fenêtre de journal en bas de la fenêtre principale. Cette fenêtre de journal est utilisée pour afficher des informations utiles sur les activités en cours, ainsi que des messages de diagnostique et d'erreur. Il existe deux listes de journal: **Information** et **Warnings/Errors**.



Pour ouvrir le menu contextuel, faites un clic droit sur la fenêtre de journal.

Boîte de Dialogue Scan Network

La boîte de dialogue **Scan Network** permet de sélectionner des ordinateurs dans un réseau et les actions à effectuer sur les postes choisis (installer ou désinstaller DeviceLock Service, affecter des autorisations, etc.).



Pour ouvrir la fenêtre de dialogue **Scan Network**, sélectionnez l'option **Scan Network** dans le menu **File** ou activez le bouton correspondant dans la barre d'outil principale (**Main toolbar**). Si vous activez la case **Show this dialog at next startup**, la boîte de dialogue **Scan Network** s'ouvrira automatiquement à chaque démarrage de DeviceLock Enterprise Manager.

Pour une gestion en réseau de DeviceLock Service, rien de plus simple: contentez-vous de suivre les trois étapes suivantes.

Sélection des ordinateurs

Commencez par sélectionner les ordinateurs qui vous intéressent.

Vous pouvez faire appel au menu contextuel, accessible par simple clic droit de votre souris, pour sélectionner/désélectionner les éléments de base (types d'ordinateurs, domaines ou ordinateurs).

DeviceLock Enterprise Manager vous propose différentes façons de faire.

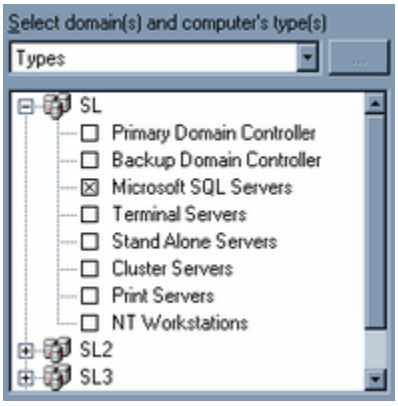
- Les ordinateurs en réseau peuvent être sélectionnés selon leurs types.

  Chaque type représente l'ensemble de tous les ordinateurs qui appartiennent à la même catégorie:

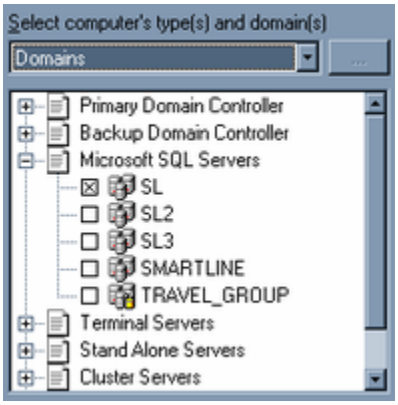
  - **Primary Domain Controller**: contrôleur de domaine primaire
  - **Backup Domain Controller**: contrôleur de domaine de sauvegarde
  - **Microsoft SQL Servers**: machines possédant un serveur Microsoft SQL Server
  - **Terminal Servers**: serveurs où s'exécutent des services de type Terminal Services
  - **Stand Alone Servers**: serveurs membres
  - **Cluster Servers**: serveurs de type cluster disponibles dans le domaine
  - **Print Servers**: serveur d'impression
  - **NT Workstations**: postes de travail sous Windows NT/2000/XP

  Le type d'ordinateur peut être choisi de deux manières:

  1. **Types**: sélectionnez le domaine de réseau, puis les types d'ordinateurs concernés.

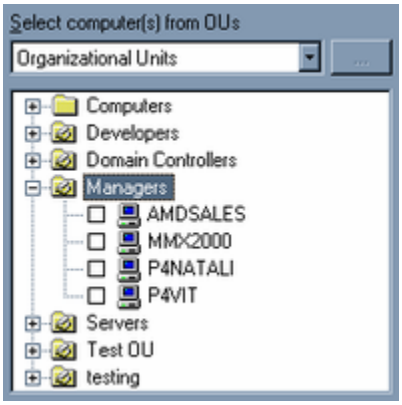
  2. **Domains**: sélectionnez le type d'ordinateur, puis les domaines de réseau dans lesquels les ordinateurs du type sélectionné doivent être pris en compte.



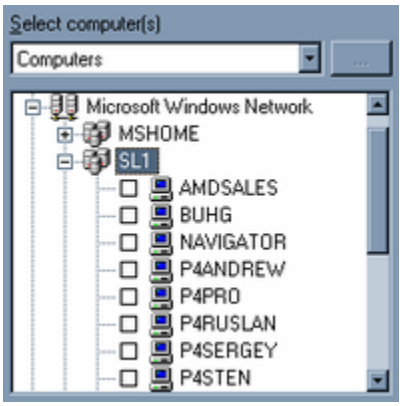
- Les ordinateurs du réseau peuvent aussi être choisis par leur nom

  Il existe plusieurs façons de choisir des ordinateurs par leur nom:

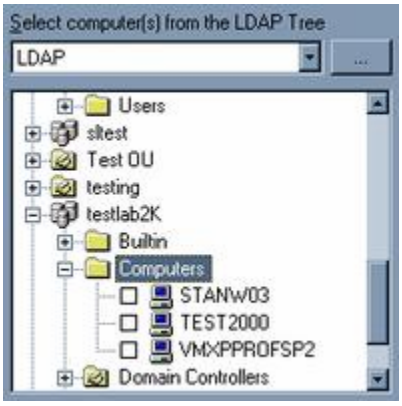
  1. **Organizational Units**: balayez la liste des Organizational Units de votre Active Directory et sélectionnez les ordinateurs qui vous intéressent.



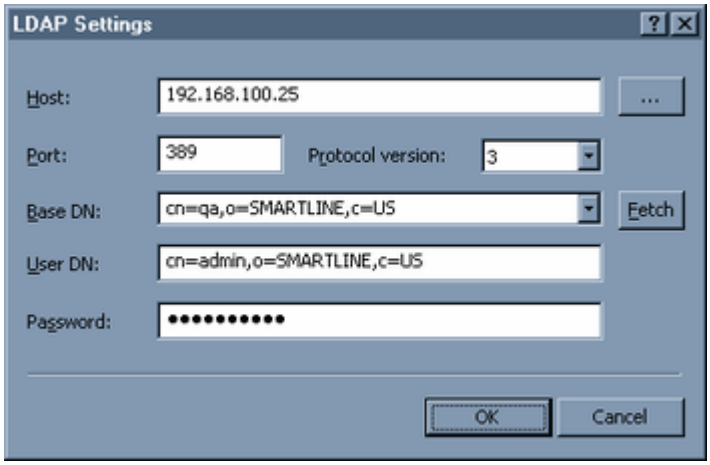
  2. **Computers**: passez en revue l'arborescence du réseau et choisissez les ordinateurs qui vous intéressent.



  3. **LDAP**: naviguez dans l'arborescence LDAP (Lightweight Directory Access Protocol) et sélectionnez les ordinateurs dans le répertoire.



Pour configurer une connexion au serveur LDAP, appuyez sur le bouton **...**.



Host: le nom ou l'adresse IP du serveur LDAP auquel il faut se connecter.

Port: le port TCP/IP sur lequel le serveur LDAP accepte des connexions. Par défaut, il s'agit du port 389.

Protocol version: la version du protocole LDAP. Certains serveurs ne sont pas totalement compatibles avec le protocole v.3 de LDAP et LDAP nécessite certaines modifications pour permettre une bonne communication avec ces serveurs. Le fait de sélectionner la **Version 2** permet de s'assurer que les requêtes de serveur sont conformes aux critères du protocole v.2 de LDAP.

Base DN: le point de départ de la navigation dans l'arborescence des répertoires. Utilisez la représentation de chaînes de LDAP pour les noms distingués (par exemple, cn=qa, o=SMARTLINE, c=US). Laissez le champ **Base DN** vierge pour commencer à naviguer depuis la racine.

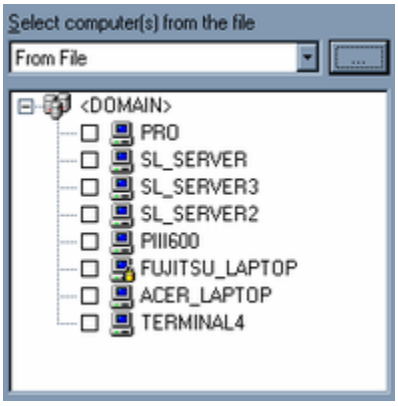
Appuyez sur le bouton **Fetch** pour obtenir tous les contextes d'attribution de noms publiés.

User DN: le nom distingué (DN) de l'utilisateur de répertoire qui permet la connexion au répertoire. Utilisez la représentation de chaînes de LDAP pour les noms distingués (par exemple, cn=qa, o=SMARTLINE, c=US).

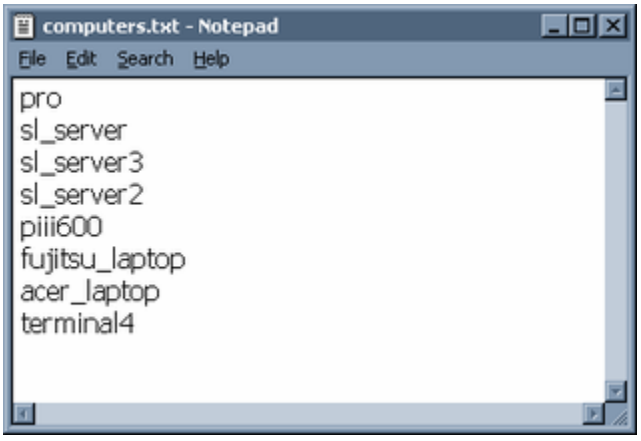
Password: le mot de passe de l'utilisateur.

4. **From File**: dans ce cas, chargez une liste d'ordinateurs prédéfinie à partir d'un fichier de texte externe puis sélectionnez les ordinateurs qui vous intéressent.

Pour ouvrir un fichier externe, appuyez sur le bouton **...**.

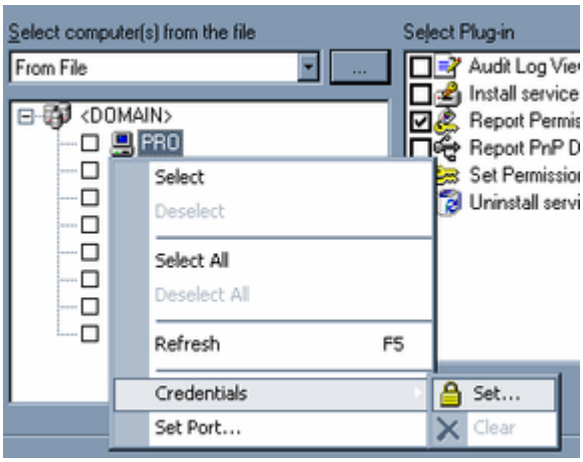


Un fichier de texte doit impérativement afficher le nom de chaque ordinateur ou son adresse IP sur des lignes séparées et peut être au format Unicode ou pas. Voici ce à quoi un fichier de texte peut ressembler:



Fourniture des accréditations

Pour attribuer d'autres accréditations aux ordinateurs cible, sélectionnez l'ordinateur ou le domaine réseau dans l'arborescence et utilisez le sous-menu **Credentials** du menu contextuel (clic droit).

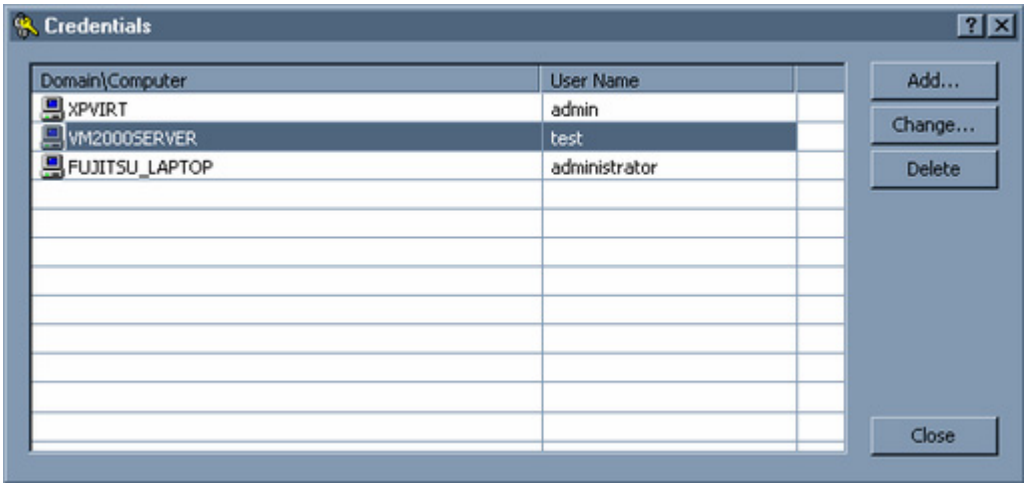


Vous pouvez attribuer des accréditations à des ordinateurs individuels et/ou à des domaines réseau. Pour ajouter des accréditations, utilisez **Set**. Pour supprimer des accréditations, utilisez **Clear**.

Les accréditations sont constituées d'une paire (nom d'utilisateur + mot de passe) servant à authentifier les ordinateurs sous contrôle. Par défaut, DeviceLock Enterprise Manager utilisera les accréditations en cours pour ouvrir automatiquement des sessions et assurer le traitement du ou des ordinateurs. Si, à ce stade, les accréditations de l'utilisateur ne disposent pas de droits administratifs sur tous les ordinateurs cible, il vous faudra fournir de nouvelles accréditations. DeviceLock Enterprise Manager utilisera ces accréditations pour ouvrir automatiquement des sessions avec les ordinateurs cible.

Dans tous les cas, les accréditations sont stockées avec des techniques de cryptage et ne sont consultables que par l'utilisateur qui possède les privilèges administratifs appropriés.

Les accréditations peuvent également être obtenues via le dialogue **Credentials**. Pour ouvrir cette boîte de dialogue, allez dans le menu **File**.

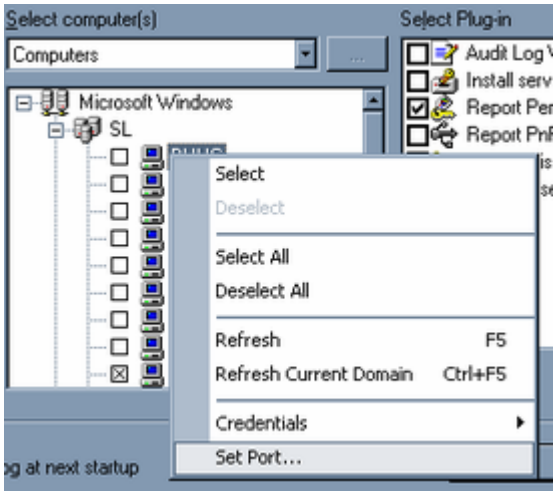


Cliquez sur **Add** pour ajouter de nouvelles accréditations. Pour changer des accréditations préexistantes, sélectionnez l'élément dans la liste et cliquez sur **Change**.

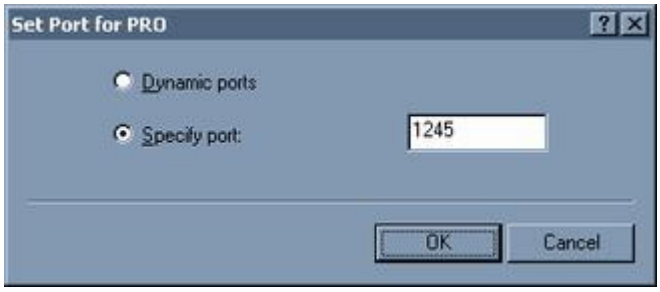
Pour supprimer des accréditations, sélectionnez l'élément dans la liste et cliquez sur **Delete**. Les touches Ctrl et/ou Maj permettent de sélectionner et de supprimer plusieurs données en même temps.

Choix du port

Vous pouvez ordonner à DeviceLock Enterprise Manager d'utiliser un port fixe, ce qui simplifie la configuration d'un Pare-feu, en cliquant tout simplement sur **Set port** dans le menu contextuel.



Par défaut, DeviceLock Enterprise Manager utilise des ports dynamiques pour la communication RPC avec DeviceLock Service. Mais si DeviceLock Service a été configuré pour accepter des connexions sur un port fixe, renseignez le paramètre **Specify port**.



Pour utiliser les ports dynamiques, cliquez sur **Dynamic ports**.

Vous pouvez configurer DeviceLock Service pour qu'il utilise soit un port fixe, soit des ports dynamiques lors du processus d'installation. Pour plus d'informations à ce sujet, veuillez vous reporter aux chapitres Installation automatique et Installation à distance via DeviceLock Enterprise Manager de ce manuel.

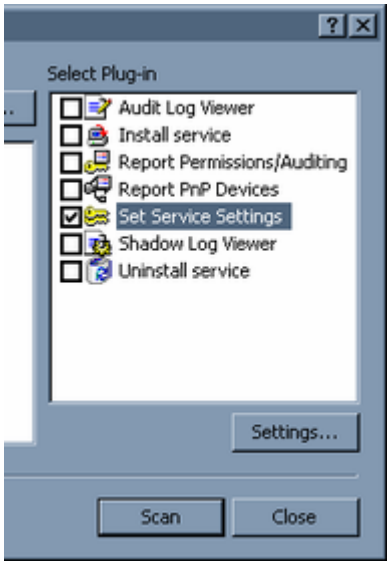
Pour changer la configuration des ports après l'installation de DeviceLock Service, utilisez l'extension Install service.

Pour savoir quels ports sont utilisés et pour quelles actions, veuillez vous reporter au chapitre Plug-ins de ce manuel.

Sélection des Plug-ins

Il vous faut maintenant choisir le plug-in qui assurera le traitement des ordinateurs en réseau que vous venez de sélectionner.

Pour sélectionner/désélectionner ces plug-ins, vous pouvez, d'un simple clic droit de votre souris, faire appel au menu contextuel.



Pour définir les paramètres du plug-in choisi, cliquez sur le bouton **Settings** situé en bas de la fenêtre de sélection des plug-ins. Si vous avez sélectionné un plug-in qui ne prend pas en charge les autres paramètres, le bouton **Settings** figurera en gris.

Les tâches sont transmises au plug-in par DeviceLock Enterprise Manager.

Le plug-in remplit les tâches et renvoie l'information à DeviceLock Enterprise Manager. A réception, DeviceLock Enterprise Manager affiche cette information sur une fenêtre séparée.

Démarrer un scan

Une fois les ordinateurs et le bon plug-in choisis, il ne vous reste plus qu'à démarrer le scan en activant le bouton **Scan**.

Dès que le scan est lancé, vous pouvez commencer à examiner l'information que vous avez déjà reçue du plug-in.

Ce scan ne monopolisera pas votre système. Vous pouvez aussi utiliser la plupart des autres fonctionnalités de DeviceLock Enterprise Manager.

Seules actions interdites durant le scan: fermer DeviceLock Enterprise Manager ou lancer un autre scan.

Si, pour une raison quelconque, vous souhaitiez interrompre le scan, cliquez sur **Stop Scan** dans le menu **File** ou activez l'icône ad-hoc de la barre d'outil principale. Le processus de scan s'interrompt dès qu'un plug-in rend le contrôle à DeviceLock Enterprise Manager.

Plug-ins

DeviceLock Enterprise Manager comporte une architecture flexible qui permet d'ajouter des modules d'extension supplémentaires (plug-ins) sur demande. DeviceLock Enterprise Manager charge les plug-ins au démarrage à partir du sous-répertoire ***Plug-ins***, qui se trouve dans le répertoire principal de DeviceLock Enterprise Manager.

DeviceLock Enterprise Manager est livré avec des plug-ins standards. Ces plug-ins nécessitent l'ouverture de certains ports sur les ordinateurs distants, comme précisé ci-dessous:

PORTS REQUIS	PLUG-INS AFFECTES
TCP 139 ou **TCP 445** **UDP 137**: ce port ne doit être ouvert que si la connexion est établie par le nom de l'ordinateur. Si vous utilisez l'adresse IP, ce port n'est pas nécessaire.	Audit Log Viewer, Report PnP Devices
TCP 139 ou **TCP 445** **UDP 137**: ce port ne doit être ouvert que si la connexion est établie par le nom de l'ordinateur. Si vous utilisez l'adresse IP, ce port n'est pas nécessaire.	Install Service, Uninstall Service
TCP 139 ou **TCP 445** **TCP 135**: ce port ne doit être ouvert que lorsque vous utilisez la connexion par **ports dynamiques**. **TCP <tous les ports supérieurs à 1024>**: ces ports ne doivent être ouverts que lorsque vous utilisez la connexion par **ports dynamiques**. **TCP <port personnalisé>**: ce port ne doit être ouvert que lorsque vous utilisez la connexion par **port fixe**. **UDP 137**: ce port ne doit être ouvert que si la connexion est établie par le nom de l'ordinateur. Si vous utilisez l'adresse IP, ce port n'est pas nécessaire.	Report Permissions/Auditing, Set Service Settings, Shadow Log Viewer

Pour des renseignements sur la manière d'utiliser la connexion par ports dynamiques ou celle par port fixe, veuillez vous reporter au chapitre Choix du port de ce manuel.

Voici les erreurs qu'un plug-in connecté à un ordinateur distant peut recevoir:

- **The product version on the client and server machines does not match (7049)**: vous essayez de vous connecter à un ordinateur qui exécute une ancienne version de DeviceLock Service. Commencez par une mise à jour de DeviceLock Service en utilisant le plug-in Install Service.
- **The network path was not found (53)**: vous essayez de vous connecter à un ordinateur inexistant (nom ou adresse IP erroné) ou qui n'est pas accessible. Vérifiez le nom d'ordinateur que vous avez spécifié. Essayez d'accéder à cet ordinateur avec Windows Explorer, et connectez-vous y à l'aide d'un outil standard d'administration Windows (de type Computer Management, Services, etc.).
  Cette erreur peut aussi survenir si le service standard Windows Server ne s'exécute pas sur l'ordinateur distant. Vérifiez le statut du service Server et démarrez-le s'il est arrêté.

D'autres erreurs de connexion sont décrites dans le chapitre Erreurs de connexion possibles du présent manuel.

Audit Log Viewer (Visionneur de journal d'audit)

Le plug-in Audit Log Viewer récupère le journal d'audit de DeviceLock dans le sous-système local de journalisation des événements Windows de l'ordinateur.

Pour définir une taille maximale du journal d'événement et spécifier ce que Windows doit faire si ce fichier est plein, allez dans **Audit Log Settings** à l'aide du menu contextuel.

Pour supprimer tous les événements du journal, cliquez sur **Clear Audit Log** dans le menu contextuel.

Pour plus d'informations, veuillez lire le chapitre Audit Log Viewer (Service) du présent manuel.

Install Service (Service d'installation)

Le plug-in Install Service permet d'installer ou de mettre à jour DeviceLock sur vos ordinateurs.

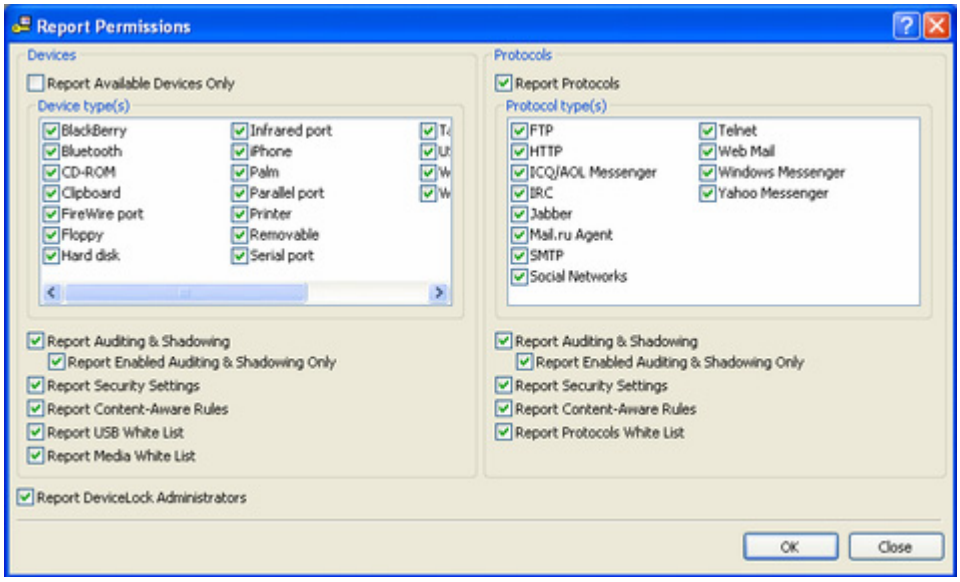
Avant de pouvoir utiliser ce plug-in, vous devez indiquer le répertoire contenant tous les fichiers nécessaires à l'installation (tels que DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe et InstMsiW.exe). Pour ce faire, cliquez sur le bouton **Settings** situé en dessous de la liste des plug-ins dans la boîte de dialogue **Scan Network** (voir Sélection des plug-ins).

Pour plus d'informations, veuillez lire le chapitre Installation à distance via DeviceLock Enterprise Manager de ce manuel.

Report Permissions/Auditing

Le plug-in Report Permissions/Auditing génère un état permettant de vérifier et de changer les politiques de sécurité définies pour les types de périphériques et pour les protocoles du réseau.

Avant de pouvoir utiliser ce plug-in, vous devez choisir les informations que vous souhaitez voir figurer dans les états. Pour ce faire, cliquez sur le bouton **Settings** situé en dessous de la liste des plug-ins dans la boîte de dialogue **Scan Network** (voir Sélection des plug-ins).



Dans la boîte de dialogue **Report Permissions**, spécifiez l'information que vous souhaitez voir figurer dans les états.

Pour recevoir les informations sur les politiques de sécurité définies pour les types de périphériques, sélectionnez les options suivantes dans **Devices**:

- **Report Available Devices Only**: en cochant cette option, vous obtenez des rapports d'autorisations uniquement pour les périphériques actuellement connectés sur l'ordinateur. Autrement, vous voyez s'afficher les autorisations et règles d'audit pour chaque type de matériel pris en charge par DeviceLock.
- **Report Auditing & Shadowing**: cochez cette option pour afficher les règles d'audit et de réplication en place.

  Lorsque cette case est cochée, vous serez informé si oui ou non le paramètre **Log Policy changes and Start/Stop events** est activé dans Service Options.
- **Report Enabled Auditing & Shadowing Only**: cochez cette option pour exclure les périphériques dont les règles d'audit et de réplication sont désactivées dans les états. Cette option n'est disponible que si le paramètre **Report Auditing & Shadowing** est coché.
- **Report Security Settings**: cochez cette option pour dresser une liste des paramètres désactivés dans Security Settings.

- **Report Content-Aware Rules**: cochez cette case pour indiquer les règles contextuelles configurées (voir Règles contextuelles pour les périphériques).
- **Report USB White List**: cochez cette option pour faire figurer les informations relatives aux matériels figurant sur la liste blanche (voir USB White List).
- **Report Media White List**: cochez cette option pour faire figurer les informations relatives aux médias figurant sur la liste blanche (voir Media White List).
- **Report DeviceLock Administrators**: cochez cette option pour afficher les comptes permettant d'administrer DeviceLock Service ou pour voir leurs configurations et leurs journaux.

Pour recevoir les informations sur les politiques de sécurité définies pour les types de périphériques, sélectionnez les options suivantes dans **Protocols**:

- **Report Protocols**: cochez cette case pour dresser une liste des politiques de sécurité pour les protocoles. Sinon, les informations concernant toutes les politiques basées sur des protocoles seront exclues des états.
  Si la case Report Protocols n'est pas cochée, les options Report Auditing & Shadowing et Report Enabled Auditing & Shadowing Only ne seront pas disponibles.
- **Report Auditing & Shadowing**: cochez cette case pour afficher les règles d'audit et de réplication définies pour les protocoles.
- **Report Enabled Auditing & Shadowing Only**: cochez cette case pour exclure les protocoles pour lesquels les règles d'audit et de réplication sont désactivées dans les états.
  Cette option n'est disponible que si la case Report Auditing & Shadowing est cochée.
- **Report Security Settings**: cochez cette case pour dresser une liste des paramètres définis par les Paramètres de sécurité.
- **Report Content-Aware Rules**: cochez cette boîte de dialogue pour dresser une liste des règles contextuelles configurées pour les protocoles (voir «Règles contextuelles pour les protocoles»).
- **Report Protocols White List**: cochez cette case pour faire figurer les informations relatives aux protocoles figurant sur la liste blanche (voir «Gestion de la liste blanche des protocoles»).

Cet état inclut toujours les informations sur le DeviceLock Certificate installé. De même, il indique systématiquement si le paramètre **Use Group Policy** est activé dans les Service Options.

Report PnP Devices (Etat des périphériques PnP)

Le plug-in Report PnP Devices génère un état où figurent à la fois les périphériques USB, FireWire et PCMCIA précédemment connectés, et ceux qui le sont actuellement sur les différents ordinateurs du réseau.

Remarque: Pour récupérer les périphériques PnP des ordinateurs sous Windows Vista/7 et Windows Server 2008, vous devez autoriser l'accès à distance à l'interface PnP sur ces ordinateurs. Pour ce faire, modifiez la politique comme indiqué dans cet article: http://support.microsoft.com/kb/947040/fr.

Les colonnes sont définies comme suit:

- **Description**: description du périphérique par le fabricant.
- **Device Information**: informations supplémentaires sur le périphérique fournies par le fabricant.
- **Connected to**: interface à laquelle le périphérique est branché (USB, FireWire ou PCMCIA).
- **Class**: classe du périphérique fournie par Windows.
- **Class description**: description de la classe du périphérique fournie par Windows.
- **Present**: indique si le périphérique est connecté ou pas (**Yes** ou **No**).
- **DeviceID**: identifiant du périphérique fourni par le fabricant.
- **Driver**: nom du gestionnaire qui contrôle le périphérique.

Vous pouvez ajouter les périphériques USB de la liste à la USB Devices Database par le biais du menu contextuel accessible à l'aide du bouton droit de la souris.

Avant de pouvoir utiliser ce plug-in, vous devez choisir les informations que vous souhaitez voir figurer dans les états. Pour ce faire, cliquez sur le bouton **Settings** situé en dessous de la liste des plug-ins dans la boîte de dialogue **Scan Network** (voir Sélection des plug-ins).

- **Report Connected Devices Only**: cochez cette option pour n'afficher que les périphériques actuellement connectés à l'ordinateur. Dans le cas contraire, vous obtiendrez la liste de tous les périphériques connectés à un moment ou à un autre à l'ordinateur.
- **Report FireWire Devices**: cochez cette option pour obtenir une liste des périphériques branchés sur le port FireWire.
- **Report PCMCIA Devices**: cochez cette option pour obtenir une liste des périphériques branchés sur le port PCMCIA.

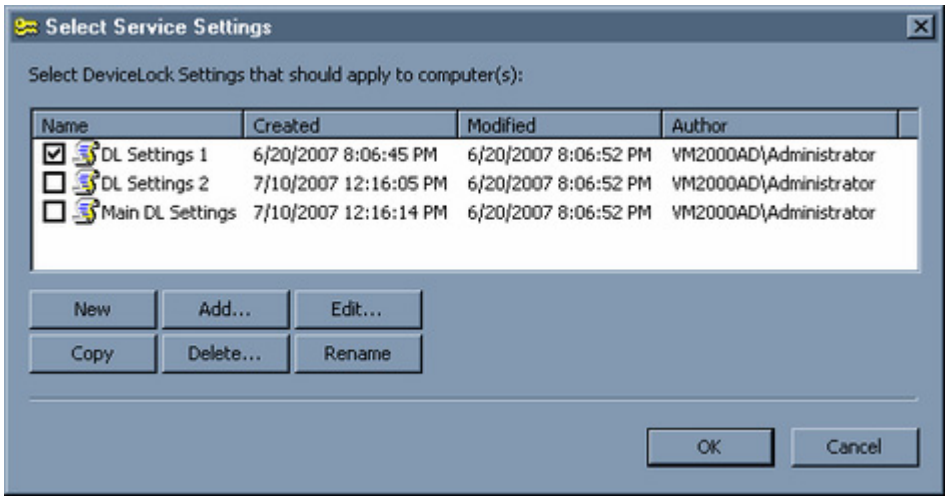
- **Report USB Devices**: cochez cette option pour obtenir une liste des périphériques branchés sur le port USB.

Set Service Settings (Définition des paramètres de service)

Le plug-in Set Service Setting lit la politique (paramètres, autorisations, règles d'audit et de réplication) à partir du fichier XML externe et la déploie dans les DeviceLock Services de l'ensemble du réseau.

Remarque: Seuls les paramètres explicitement définis dans un fichier de politiques s'appliquent aux postes client. Tous les paramètres ayant le statut **Not Configured** sont ignorés par les ordinateurs client.

Avant de pouvoir utiliser ce plug-in, vous devez spécifier la configuration, les autorisations et/ou les règles d'audit que vous souhaitez déployer. Pour ce faire, cliquez sur le bouton **Settings** situé en dessous de la liste des plug-ins dans la boîte de dialogue **Scan Network** (voir Sélection des plug-ins).



Vous devez d'abord préparer la politique que vous voulez diffuser.

Si la liste ne contient aucun fichier, vous pouvez créer un fichier vide en cliquant sur **New** ou ajouter un fichier existant en appuyant sur **Add**.

Mettez ensuite le fichier en surbrillance dans la liste et cliquez sur **Edit** pour ouvrir DeviceLock Service Settings Editor. DeviceLock Service Settings Editor sert à créer et modifier des fichiers XML externes avec les paramètres, les autorisations et les règles d'audit et de réplication nécessaires pour DeviceLock Service. Pour plus d'informations, veuillez consulter la section DeviceLock Service Settings Editor du présent manuel.

Lorsque vous avez terminé de modifier la politique, choisissez un nom de fichier dans la liste en cochant la case adjacente. Cliquez ensuite sur **OK** pour fermer la boîte de dialogue de

configuration.

Shadow Log Viewer (Visionneur de journal de replication)

Le plug-in Shadow Log Viewer récupère le journal de réplication à partir de DeviceLock Service.

Utilisez le menu contextuel disponible d'un simple clic droit pour accéder à toutes les fonctionnalités de ce plug-in.

Pour plus d'informations, veuillez lire le chapitre Shadow Log Viewer (Service) de ce manuel.

Uninstall Service (Service de désinstallation)

Le plug-in Uninstall Service supprime DeviceLock Service avec tous ses composants et tous les paramètres qui s'y rapportent.

Si DeviceLock Enterprise Manager est connecté avec un compte d'utilisateur qui ne dispose pas d'un accès administratif complet à DeviceLock Service, le plug-in ne peut pas supprimer le service.

De même, une erreur a lieu si l'utilisateur n'a pas de privilèges administratifs locaux sur l'ordinateur qui exécute DeviceLock Service.

Ouverture / Sauvegarde / Export

DeviceLock Enterprise Manager peut stocker toute les informations reçues des plug-ins.

Les données sont enregistrées dans des fichiers externes, qui peuvent être chargés sur demande dans DeviceLock Enterprise Manager à tout moment.

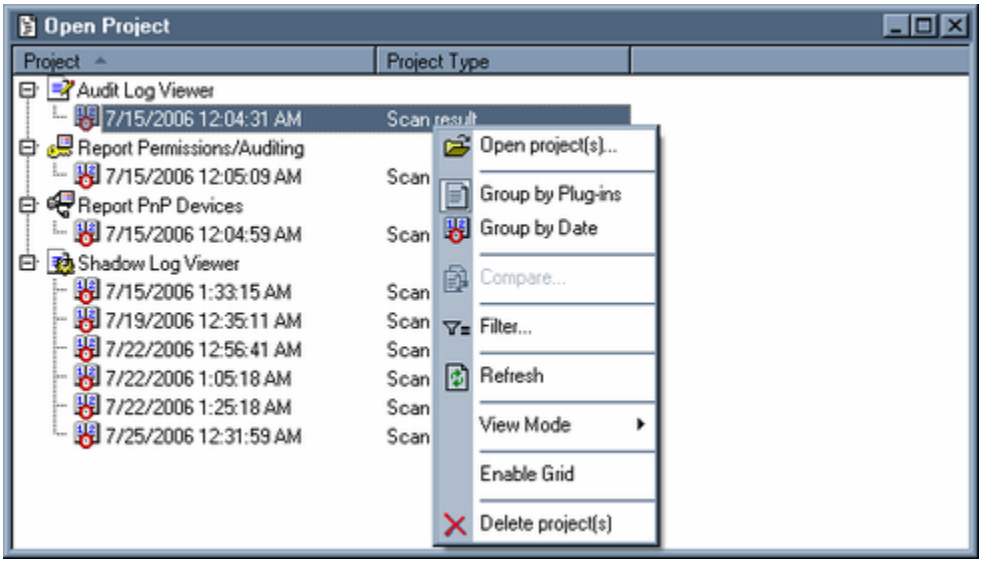
Il y a 3 façons de sauvegarder et de charger des données:

1. La méthode la plus pratique de stocker l'information reçue est de l'enregistrer comme un «projet». Lorsque vous enregistrez des données en mode projet, DeviceLock Enterprise Manager enregistre chaque fenêtre active du plug-in dans un fichier séparé de son propre format et met ce fichier dans le sous-répertoire ***Project***.

   Les noms des fichiers projet sont générés automatiquement et sont construits à partir des noms du plug-in et de la date et heure auxquelles le scan a commencé.

   Pour enregistrer des données en tant que projet, sélectionnez **Save Project** dans le menu **File** ou cliquez sur l'icône correspondante dans la barre d'outils principale.

Pour charger des projets déjà enregistrés, sélectionnez **Open Project** dans le menu **File**.



La fenêtre **Open Project** possède sa propre barre d'outils et son menu contextuel.

Vous pouvez regrouper plusieurs projets enregistrés par date de scan ou par le type d'information qu'ils contiennent. Sélectionnez **Group by Plug-ins** ou **Group by Date** dans le menu contextuel ou cliquez sur l'icône appropriée dans la barre d'outils **Project**.

Pour ouvrir un projet enregistré, sélectionnez-le dans la liste et cliquez sur l'icône **Open Project** dans la barre d'outils **Project**. Tapez Ctrl et/ou Maj pour sélectionner et ouvrir plusieurs projets en même temps.

2. Une autre façon de sauvegarder l'information reçue au format de DeviceLock Entreprise Manger est de sélectionner **Save as** dans le menu **File**. Ceci permet d'enregistrer sous le nom de votre choix un fichier de type ANM n'importe où sur votre disque dur ou sur tout autre media.

   Pour charger des fichiers enregistrés, sélectionnez **Open** dans le menu **File** ou cliquez sur l'icône appropriée dans la barre d'outils principale. Il vous sera alors demandé de spécifier le fichier que vous voulez ouvrir. Vous ne pouvez charger que des fichiers de type ANM.

3. Si vous avez besoin de transférer des informations reçues par DeviceLock Enterprise Manager à une application tierce, vous pouvez les exporter dans un fichier externe, puis les importer dans cette application. Pour exporter des données dans un fichier externe, sélectionnez **Save As** dans le menu **File**, puis choisissez le type de fichier dans **Save as** type. DeviceLock Enterprise Manager accepte les exportations au format MS Excel (si le logiciel est installé sur l'ordinateur local) et deux formats de fichier textes: TXT (séparé par des tabulations) ou CSV (séparé par des points-virgules).

   Si vous exportez des informations dans un fichier externe de type texte, vous ne pourrez pas les réimporter dans DeviceLock Enterprise Manager, dans la mesure où DeviceLock Enterprise Manager ne peut ouvrir et charger que des fichiers enregistrés dans son format. Cependant, le fait de pouvoir exporter des informations dans un fichier externe reste utile pour échanger des données entre DeviceLock Enterprise

Manager et d'autres applications.

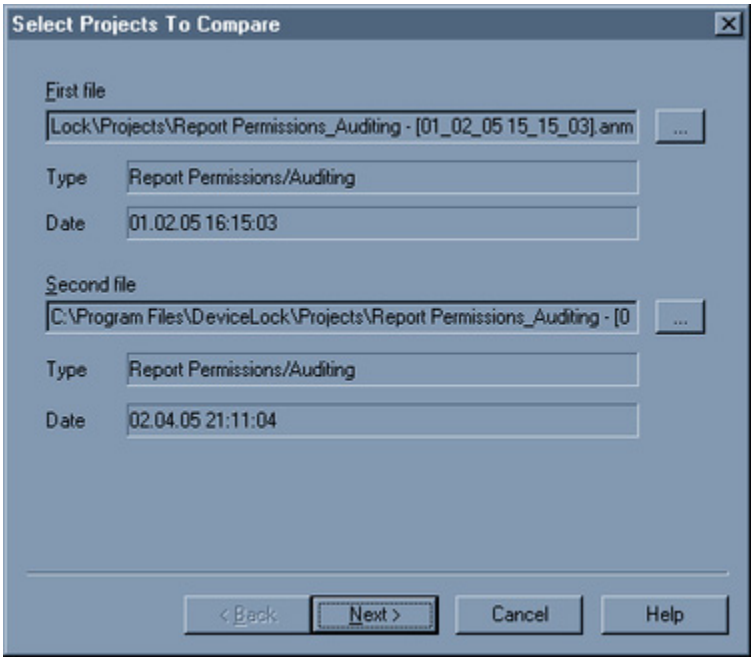
Comparaison de données

DeviceLock Enterprise Manager permet de surveiller les changements qui se produisent sur les ordinateurs du réseau en comparant deux projets sauvegardés. Le fait de surveiller ces changements est important lorsque l'on gère un nombre important de machines dans son réseau.

DeviceLock Enterprise Manager propose un assistant intuitif très utile pour comparer les fichiers ANM. Pour ouvrir cet assistant, cliquez sur **Compare** dans le menu **File**.

Pour comparer deux fichiers avec l'assistant Compare Wizard, il suffit de suivre les trois étapes suivantes:

1. Commencez par sélectionner les fichiers à comparer.

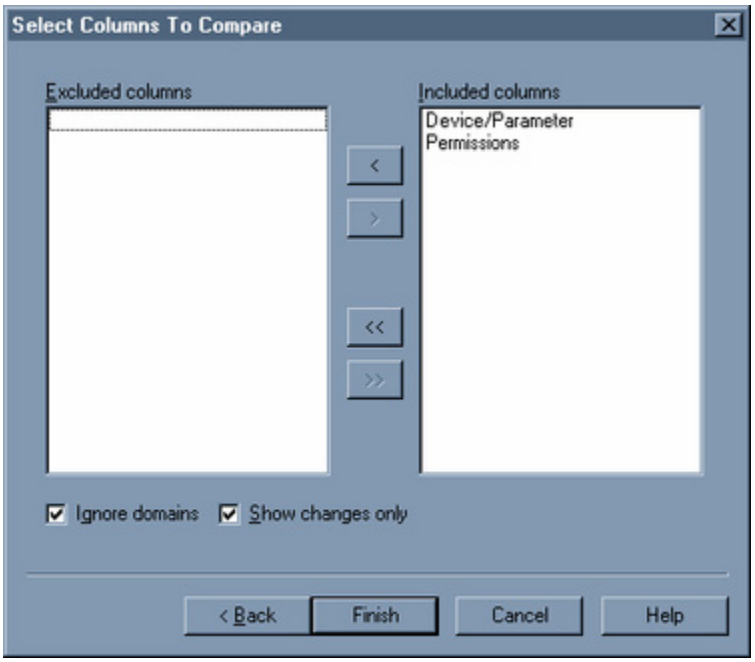


   Sélectionnez le premier fichier, puis le second en cliquant sur les icônes.

   Veuillez noter que vous ne pouvez comparer que des fichiers du même type. Par exemple, il est impossible de comparer les informations reçues du plug-in Report Permissions/Auditing avec des informations provenant du plug-in Report PnP Devices.

   Une fois les deux fichiers sélectionnés, cliquez sur **Next** pour vous rendre sur la page suivante de l'assistant.

2. La seconde étape consiste à sélectionner les colonnes que vous souhaitez inclure dans la procédure de comparaison des données.



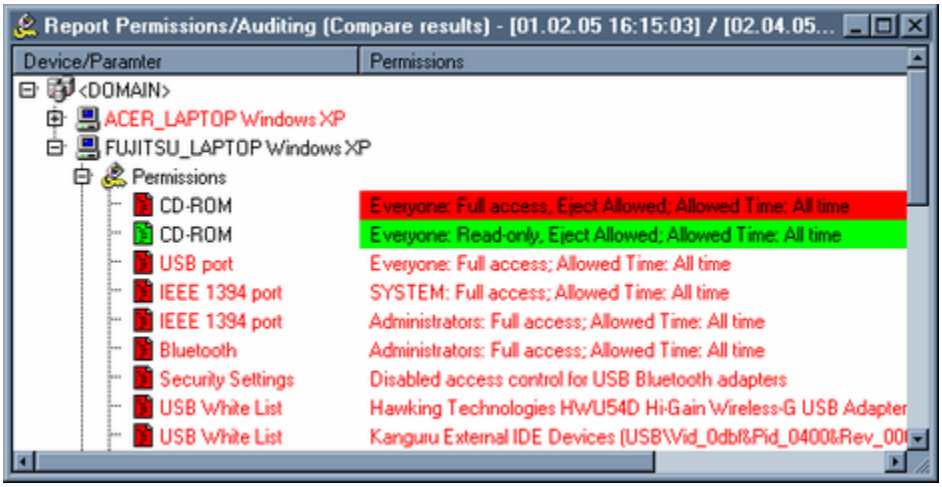
DeviceLock Enterprise Manager ne comparera que les colonnes que vous aurez sélectionnées. Si vous avez besoin d'exclure une colonne de la comparaison, transférez-la de la liste des **Included columns** vers celle des **Excluded columns**. Les colonnes exclues seront visibles dans le résultat comparatif mais les valeurs qu'elles contiennent seront ignorées et n'affecteront pas le résultat des comparaisons.

Par défaut, les résultats comparatifs affichés ne concerneront que les informations qui sont différentes dans les deux fichiers. Pour voir tous les enregistrements (même ceux qui n'ont pas changé), désactivez la case **Show changes only**.

Pour inclure les noms des domaines du réseau dans la procédure de comparaison, désactivez la case **Ignore domains**. Lorsque la case **Ignore domains** est cochée, DeviceLock Enterprise Manager ignore les domaines et ne compare que les ordinateurs et les informations contenues dans ces ordinateurs.

3. La troisième et dernière étape consiste à démarrer la procédure de comparaison. Cliquez sur l'icône **Finish** pour comparer les deux fichiers sélectionnés.

   DeviceLock Enterprise Manager affiche les résultats comparatifs dans une fenêtre séparée sous la forme d'une arborescence, exactement comme il affiche les informations reçues des plug-ins.


Report Permissions/Auditing (Compare results) - [01.02.05 16:15:03] / [02.04.05...
Device/Paramter
Permissions
<DOMAIN>
ACER_LAPTOP Windows XP
FUJITSU_LAPTOP Windows XP
Permissions
CD-ROM
Everyone: Full access, Eject Allowed; Allowed Time: All time
CD-ROM
Everyone: Read-only, Eject Allowed; Allowed Time: All time
USB port
Everyone: Full access; Allowed Time: All time
IEEE 1394 port
SYSTEM: Full access; Allowed Time: All time
IEEE 1394 port
Administrators: Full access; Allowed Time: All time
Bluetooth
Administrators: Full access; Allowed Time: All time
Security Settings
Disabled access control for USB Bluetooth adapters
USB White List
Hawking Technologies HWU54D Hi-Gain Wireless-G USB Adapter
USB White List
Kanguru External IDE Devices (USB\Vid_0dbf&Pid_0400&Rev_00

La comparaison est aussi simple qu'efficace:

1. Si la case **Ignore domains** n'est pas cochée, le programme énumère les domaines réseau des deux fichiers sélectionnés et essaye de trouver chaque domaine à la fois dans le fichier le plus ancien et le plus récent.

   Si le domaine existe dans le fichier le plus ancien mais pas dans le plus récent, DeviceLock Enterprise Manager insère le domaine qui manque (ainsi que tous les ordinateurs compris dans ce domaine et les informations de ces ordinateurs) dans le résultat comparatif, puis note tous les enregistrements en rouge.

   Si le domaine n'existe pas dans le fichier le plus ancien mais existe dans le plus récent, DeviceLock Enterprise Manager insère le domaine qui manque (ainsi que tous les ordinateurs compris dans ce domaine, et les informations de ces ordinateurs) dans le résultat comparatif, puis note tous les enregistrements en vert.

   Si le domaine existe dans les deux fichiers, DeviceLock Enterprise Manager énumère tous les ordinateurs contenus dans le domaine (voir ci-dessous).

2. Si la case **Ignore domains** est cochée, DeviceLock Enterprise Manager ignore les domaines et énumère tous les ordinateurs dans les deux fichiers sélectionnés et essaye de trouver chaque machine à la fois dans le fichier le plus ancien et le plus récent.

   SI l'ordinateur existe dans le fichier le plus ancien mais pas dans le plus récent, DeviceLock Enterprise Manager insère l'ordinateur manquant avec toutes les informations qu'il contient dans le résultat comparatif et note tous les enregistrements en rouge.

   SI l'ordinateur n'existe pas dans le fichier le plus ancien mais existe dans le plus récent, DeviceLock Enterprise Manager insère l'ordinateur manquant avec toutes les informations qu'il contient dans le résultat comparatif et note tous les enregistrements en vert.

   Si l'ordinateur existe dans les deux fichiers, DeviceLock Enterprise Manager énumère toutes les informations qu'il contient (voir-ci-dessous).

3. DeviceLock Enterprise Manager énumère toutes les informations de l'ordinateur et essaie de trouver tous les enregistrements, à la fois dans le fichier le plus récent et le plus ancien.

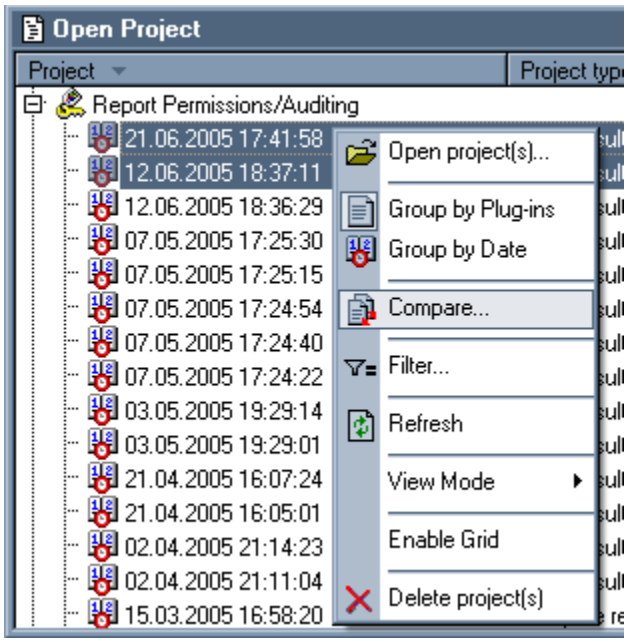
Si l'enregistrement existe dans le fichier le plus ancien mais pas dans le plus récent, DeviceLock Enterprise Manager insère l'enregistrement manquant dans le résultat comparatif et le note en rouge.

Si l'enregistrement n'existe pas dans le fichier le plus ancien mais existe dans le fichier le plus récent, DeviceLock Enterprise Manager insère l'enregistrement manquant dans le résultat comparatif et le note en vert.

Si l'enregistrement existe dans les deux fichiers, DeviceLock Enterprise Manager commence à comparer chacune des colonnes incluses pour cet enregistrement:

- Si les valeurs des colonnes sont différentes pour le fichier le plus ancien et le plus récent, DeviceLock Enterprise Manager insère les deux enregistrements dans le résultat comparatif. L'enregistrement du fichier le plus récent est présenté juste après celui du fichier le plus ancien.
  La colonne qui appartient à l'enregistrement le plus ancien est surlignée en rouge. Celle qui appartient à l'enregistrement récent est surlignée en vert. Toutes les colonnes qui ont été exclues, ainsi que les colonnes qui ont des valeurs égales sont non surlignées et sont affichées dans la couleur par défaut.
- Si toutes les colonnes des enregistrements des deux fichiers ont des valeurs identiques, DeviceLock Enterprise Manager ou bien n'affiche rien (la case **Show changes only** est cochée), ou bien insère cet enregistrement dans le résultat comparatif et l'affiche dans la couleur par défaut (la case **Show changes only** n'est pas cochée).

Pour comparer deux fichiers que vous avez sauvegardés comme projets, le mieux est d'utiliser la fonctionnalité spéciale de la fenêtre **Open Project**.



Choisissez **Open Project** dans le menu **File**, sélectionnez les deux projets que vous souhaitez comparer (tapez sur Ctrl et/ou Shift pour sélectionner deux projets en même temps), puis sélectionnez **Compare** dans le menu contextuel ou cochez l'icône appropriée dans la barre d'outils **Project**.

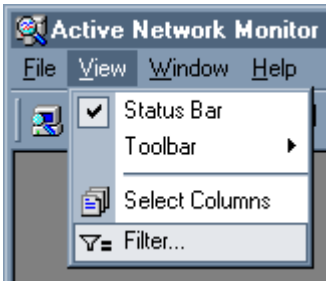
Veuillez noter que vous ne pouvez choisir que deux projets, et que ceux: ci doivent être du même type.

DeviceLock Enterprise Manager propose deux icônes sur la barre d'outils **Compare**, destinés à vous aider à naviguer facilement dans les résultats comparatifs. Cliquez sur le bouton **<** pour sélectionner l'enregistrement précédent dans le résultat comparatif qui contient les changements. Cliquez sur le bouton **>** pour sélectionner l'enregistrement suivant dans le résultat comparatif qui contient les changements.

Vous pouvez également enregistrer le résultat comparatif dans un fichier extérieur au format ANM ou l'exporter en format MS Excel ou texte (TXT ou CSV). Cliquez sur **Save As** dans le menu **File** ou cliquez sur l'icône correspondante dans la barre d'outils principale pour enregistrer ou exporter le résultat comparatif.

Comme pour tous les autres fichiers DeviceLock Enterprise Manager, le résultat comparatif peut être ouvert et chargé dans DeviceLock Enterprise Manager. Pour charger un résultat comparatif sauvegardé, cliquez sur **Open** dans le menu **File** ou l'icône correspondante de la barre d'outils principale. Il vous sera alors demandé de spécifier le fichier que vous voulez ouvrir. Vous ne pouvez charger que des fichiers de type ANM.

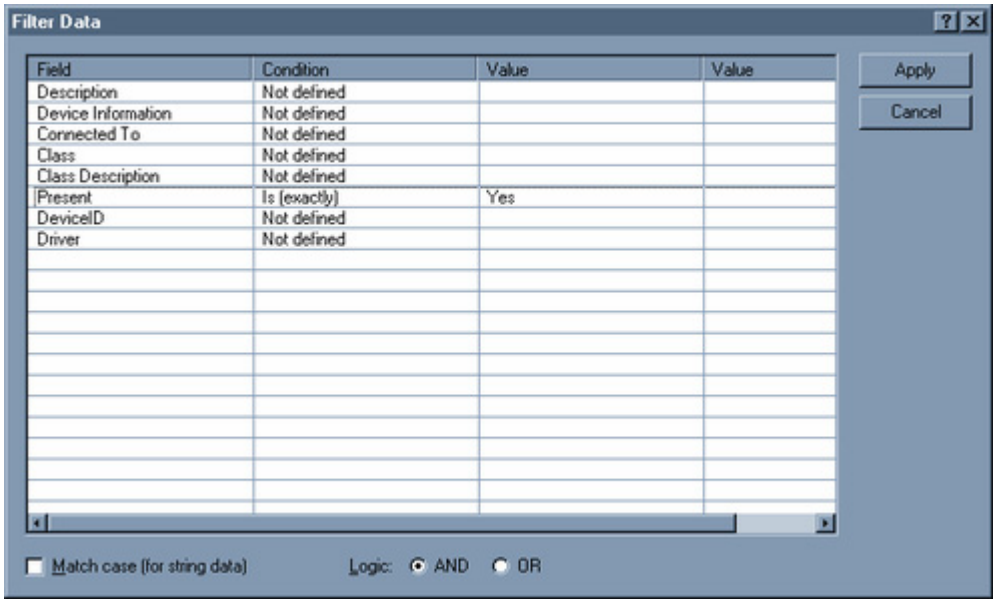
Filtrage de données



DeviceLock Enterprise Manager comporte un outil de filtrage de données très sophistiqué, qui permet de circonscrire précisément votre scan ou vos résultats comparatifs aux seules données qui remplissent vos conditions.

Pour ouvrir la boîte de dialogue **Filter Data**, sélectionnez **Filter** dans le menu **View** ou cliquez sur l'icône correspondante dans la barre d'outils principale.

Veuillez noter que la fenêtre avec un scan ou une comparaison doit être active pour faire l'objet d'un filtrage de données.



- La colonne **Field** contient tous les champs disponibles dans le scan ou le résultat comparatif que vous voulez filtrer. Vous pouvez définir la logique **AND/OR** séparément pour chaque champ.

  AND: n'inclut que les enregistrements qui satisfont toutes les conditions requises. Par exemple, Process = "explorer.exe" AND PID = 3764 récupère toutes les données où la procédure Process est "explorer.exe" et l'identifiant PID est 3764. Il n'inclut pas les données qui ne satisfont qu'à l'une de ces deux conditions.

  OR: inclut tous les enregistrements qui satisfont au moins une condition. Par exemple Process = "explorer.exe" OR PID = 3764 récupère toutes les données où l'une ou bien les deux conditions suivantes sont satisfaites : la procédure = "explorer.exe" (quel que soit l'identifiant PID) ou bien l'identifiant PID = 3764 (quelle que soit la procédure).

- La colonne **Condition** contient la liste des opérations logiques que vous pouvez effectuer dans un champ sélectionné. Vous ne pouvez choisir qu'une seule opération logique par champ. DeviceLock Enterprise Manager accepte deux groupes d'opérations logiques, pour les string data et les non-string data.

  Les opérations logiques qui peuvent être effectuées sur des données string (target string étant la chaîne de caractères que vous spécifiez, par ex. "Explorer.exe"):

  - **Is (exactly)**: sélectionne uniquement les données qui comportent des champs avec des chaînes identiques à la chaîne cible.
  - **Includes**: sélectionne uniquement les données qui comportent des champs qui incluent une chaîne cible définie.
  - **Is not**: sélectionne uniquement les données dont les champs ayant des chaînes sont différents de la chaîne cible.
  - **Not includes**: sélectionne uniquement les données qui comportent des champs avec des chaînes qui n'incluent pas la chaîne cible.
  - **Empty**: sélectionne uniquement les données dont les champs comportent des chaînes vides.
  - **Not Empty**: sélectionne uniquement les données dont les champs comportent des chaînes qui ne sont pas vides.
  - **Regular expression**: sélectionne uniquement les données dont les champs ont des chaînes qui correspondent à une expression. L'expression peut contenir des jokers (par ex: "explorer*").

  Pour que votre recherche fasse la différence entre les majuscules et les minuscules (ex: "Explorer.exe" considéré comme différent de "explorer.exe"), cochez la case **Match case**. Dans le cas contraire, la différence entre majuscules et minuscules ne sera pas prise en compte.

  Les opérations logiques peuvent également être effectuées sur des données non-string:

  - **Equal to (=)**: sélectionne les données dont les valeurs de champ sont identiques à la valeur définie (ex: PID = 3764).
  - **Greater than (>)**: sélectionne les données dont les valeurs sont plus grandes que la valeur définie (ex: PID > 4).
  - **Less than (<)**: sélectionne les données dont les valeurs sont plus petites que la valeur définie (ex: PID < 4).

- **Not Equal to (!=)**: sélectionne les données dont les valeurs de champ sont différentes de la valeur définie (ex: PID != 0).
- **Between (in)**: sélectionne les données dont les valeurs de champ se situent entre les deux valeurs définies (ex: PID entre 3000-4000).
- **Not Between (out)**: sélectionne les données dont les valeurs de champ se situent en dehors des deux valeurs définies (ex: PID non compris dans entre 3000-4000).
- **Regular expression**: sélectionne uniquement les données dont les valeurs de champ correspondent à une expression. Cette expression peut contenir des jokers (ex: 300*).

Si vous ne souhaitez pas effectuer une opération logique pour un champ déterminé, sélectionnez **Not defined** dans la liste des opérations logiques.

- Les colonnes **Value** contiennent les arguments logiques définis par l'utilisateur. La seconde colonne **Value** est utilisée uniquement dans le cas où les opérations de type **Between (in)** ou **Not Between (out)** sont sélectionnées. Pour toutes les autres opérations logiques, seule la première colonne est nécessaire.

Une fois l'expression-filtre définie, cliquez sur **Apply** pour commencer la procédure de filtrage.

Vous pouvez sauvegarder votre résultat dans un fichier externe de type ANM ou l'exporter dans un fichier de texte (TXT et CSV) ou encore MS Excel. Pour ce faire, cliquez sur **Save As** dans le menu **File** ou sélectionnez l'icône correspondante dans la barre de menu principale (**Main toolbar**).

Comme pour tous les fichiers générés par DeviceLock Enterprise Manager, les données filtrées peuvent être ouvertes et chargées dans DeviceLock Enterprise Manager. Pour charger un fichier, cliquez sur **Open** dans le menu **File**, ou sélectionnez l'icône correspondante dans la barre de menu principale. Indiquez ensuite le fichier que vous souhaitez ouvrir. Vous ne pouvez charger que des fichiers qui ont été précédemment sauvegardés par DeviceLock Enterprise Manager.

Règles contextuelles pour les périphériques (Regular Profile)

Les règles contextuelles étendent les fonctions de contrôle d'accès aux ports et aux périphériques de base de DeviceLock en y apportant une protection supplémentaire, intuitive et au niveau du fichier, des documents d'entreprise contenant des informations confidentielles sur la société. Les règles contextuelles activent la vérification automatique du contenu des données copiées vers des périphériques de stockage externes, la détection des contenus sensibles et l'application des politiques réglementaires afin de garantir la protection des données.

Les règles contextuelles permettent d'accorder ou de refuser, de manière sélective, l'accès à certains contenus, indépendamment des permissions préétablies au niveau typologique. Les règles contextuelles permettent également d'accorder ou de refuser la copie de réplication de certains contenus. Pour plus de flexibilité, les Règles contextuelles peuvent être définies au niveau de l'utilisateur ou au niveau du groupe.

Vous pouvez configurer les règles contextuelles pour qu'elles s'appliquent aux opérations de contrôle d'accès, à celles de copie de réplication, ou aux deux.

Voici quelques exemples d'utilisation des règles contextuelles.

- **Exemple 1 – Utilisation des règles contextuelles pour opérations de contrôle d'accès**. Vous pouvez accorder à certains utilisateurs ou groupes d'utilisateurs le droit de lire des fichiers contenant l'expression «ne pas distribuer» à partir de périphériques amovibles, de disquettes ou de CD/DVD, tout en leur refusant le droit d'écrire des fichiers contenant plus d'un numéro de carte de crédit sur des périphériques amovibles ou des disquettes.
- **Exemple 2 – Utilisation des règles contextuelles pour opérations de copie de réplication**. Vous pouvez définir des règles n'autorisant que les fichiers contenant des numéros de cartes de crédit, des numéros de sécurité sociale, les mots «secret», «confidentiel», «restreint», les expressions «Top secret» et «Pour utilisation officielle uniquement» pour la copie de réplication à des fins d'audit de sécurité et d'enquêtes sur les incidents.

Remarque: Vous pouvez définir des règles contextuelles différentes selon qu'il s'agit de règles Online (en ligne) ou Offline (hors ligne) pour le même utilisateur ou groupe d'utilisateurs. Les règles contextuelles en ligne (Regular Profile) s'appliquent aux ordinateurs client qui travaillent en ligne. Les règles contextuelles hors ligne (Regular Profile) s'appliquent aux ordinateurs client qui travaillent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, consultez le chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur la façon de définir les Offline règles contextuelles, consultez le chapitre intitulé «Gestion des règles contextuelles hors ligne pour les périphériques.»

Règles contextuelles pour opérations de contrôle d'accès

Lorsqu'elles s'appliquent à des opérations de contrôle d'accès, les règles contextuelles contrôlent les opérations de copie, d'écriture et de suppression des contenus spécifiés. Le contrôle des opérations de suppression et d'écriture se fait simultanément.

Les règles contextuelles permettent d'effectuer les opérations suivantes:

- Accorder l'accès en lecture/écriture au contenu de fichier indiqué lorsque l'accès est refusé au niveau typologique.
- Refuser l'accès en lecture/écriture au contenu de fichier indiqué lorsque l'accès est accordé au niveau typologique.

Remarque: DeviceLock peut vérifier l'accès aux périphériques à deux niveaux: au niveau de l'interface (le port) et au niveau du type. Certains périphériques sont soumis à des vérifications aux deux niveaux, d'autres à un seul. Par exemple, une clé USB appartient aux deux niveaux: interface (USB) et type (Removable). Les règles contextuelles ne fonctionnent que lorsque la vérification d'accès a lieu au niveau du type (Removable, Floppy, etc.). DeviceLock n'effectue pas le contrôle d'accès des périphériques USB au niveau du type si les conditions suivantes sont vérifiées:

- le périphérique n'est pas ajouté à la USB Devices White List, l'option **Access control for USB storage devices** est activée dans les Security Settings et l'utilisateur n'a pas accès aux périphériques de type ports USB.
OU
- le périphérique est ajouté à la USB Devices White List et la case **Control As Type** est décochée pour ce faire.

Le tableau suivant contient un résumé des droits d'accès susceptibles d'être indiqués dans les règles contextuelles.

DROITS D'ACCES	DESCRIPTION
Generic: Read	Contrôle si l'utilisateur peut lire le contenu spécifié à partir d'un périphérique. S'applique aux périphériques de types DVD/CD–ROM, Floppy, et Removable.
Generic: Write	Contrôle si l'utilisateur peut écrire le contenu spécifié sur un périphérique. S'applique aux périphériques de types Floppy et Removable.
Generic: Read, Write	Contrôle si l'utilisateur peut lire et écrire le contenu spécifié sur un périphérique donné. S'applique aux périphériques de types Floppy et Removable.
Encrypted: Read	Contrôle si l'utilisateur peut lire le contenu spécifié sur un périphérique crypté. Ne s'applique qu'aux dispositifs de type Removable.
Encrypted: Write	Contrôle si l'utilisateur peut écrire le contenu spécifié sur un périphérique crypté. Ne s'applique qu'aux dispositifs de type Removable.
Encrypted: Read, Write	Contrôle si l'utilisateur peut lire et écrire le contenu spécifié sur un périphérique crypté. Ne s'applique qu'aux dispositifs de type Removable.

Remarque: Les droits d'accès génériques indiqués pour les périphériques de type Removable ne s'appliquent qu'aux périphériques non cryptés. Les droits d'accès cryptés indiqués pour les périphériques de type Removable ne s'appliquent qu'aux périphériques cryptés. Pour indiquer des droits d'accès aux périphériques Removable tant cryptés que non cryptés, veuillez indiquer des droits d'accès tant Generic que Encrypted. Pour en savoir plus sur les périphériques qui sont reconnus par DeviceLock Service en tant que périphériques cryptés, veuillez consulter le chapitre intitulé «Encryption (Cryptage).»

Le tableau suivant montre en quoi les différentes permissions au niveau du type de périphérique et au niveau du fichier affectent l'état d'une permission pour un compte d'utilisateur donné. Les permissions au niveau du type de périphérique sont des permissions accordées pour un type de périphérique. Les permissions au niveau du fichier sont des permissions définies par les règles contextuelles.

	FULL ACCESS niveau type de périphérique	**NO ACCESS** niveau type de périphérique	**ALLOW READ/ DENY WRITE** niveau type de périphérique
ALLOW READ niveau fichier	accorde l'accès en lecture à tous les contenus, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture uniquement aux contenus indiqués, empêche la création et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture à tous les contenus, empêche la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
DENY READ niveau fichier	refuse l'accès en lecture aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	refuse l'accès à un périphérique.	refuse l'accès en lecture aux contenus indiqués, empêche la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
ALLOW WRITE niveau fichier	accorde l'accès en écriture à tous les contenus, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
DENY WRITE niveau fichier	refuse l'accès en écriture aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	refuse l'accès à un périphérique.	refuse l'accès en écriture aux contenus indiqués, empêche la création, la suppression et le changement de nom des fichiers de zéro (0) octet.

	FULL ACCESS niveau type de périphérique	**NO ACCESS** niveau type de périphérique	**ALLOW READ/ DENY WRITE** niveau type de périphérique
ALLOW READ/ ALLOW WRITE niveau fichier	accorde l'accès en lecture et en écriture à tous les contenus, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture et en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture à tous les contenus, accorde l'accès en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
DENY READ/ DENY WRITE niveau fichier	refuse l'accès en lecture et en écriture aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	refuse l'accès à un périphérique.	refuse l'accès en lecture aux contenus indiqués, refuse l'accès en écriture à tous les contenus, empêche la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
ALLOW READ/ DENY WRITE niveau fichier	accorde l'accès en lecture à tous les contenus, refuse l'accès en écriture aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture uniquement aux contenus indiqués, refuse l'accès en écriture à tous les contenus, empêche la création et le changement de nom des fichiers de zéro (0) octet.	accorde l'accès en lecture à tous les contenus, refuse l'accès en écriture à tous les contenus, empêche la création, la suppression et le changement de nom des fichiers de zéro (0) octet.
DENY READ/ ALLOW WRITE niveau fichier	refuse l'accès en lecture aux contenus indiqués, accorde l'accès en écriture à tous les contenus, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	refuse l'accès en lecture à tous les contenus, accorde l'accès en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.	refuse l'accès en lecture aux contenus indiqués, accorde l'accès en écriture uniquement aux contenus indiqués, permet la création, la suppression et le changement de nom des fichiers de zéro (0) octet.

Remarque: Si la permission No Access est définie pour un type de périphériques et qu'il existe une règle contextuelle qui permet l'accès en écriture à certains contenus pour le même type de périphériques, la permission Traverse Folder est accordée aux utilisateurs pour ce type de périphériques. La permission Traverse Folder permet à l'utilisateur de se déplacer dans les dossiers et

de voir les fichiers et les dossiers situés dans les sous-répertoires, même si l'utilisateur n'est pas autorisé à lire les dossiers rencontrés.

Tenez compte des points suivants lors de l'utilisation des règles contextuelles:

- ***Si les règles contextuelles sont définies à la fois pour les périphériques et pour les protocoles, toutes les vérifications d'accès seront exécutées en un seul traitement***.
- ***Les règles contextuelles avec paramètres Refuser sont prioritaires par rapport aux règles avec paramètres Autoriser si elles s'appliquent au même utilisateur ou groupe d'utilisateurs***.
- ***Si des utilisateurs tentent d'écraser un fichier existant à l'aide d'un nouveau fichier auquel ils n'ont pas le droit d'accéder, l'ancien fichier est supprimé.***
- ***Si des utilisateurs tentent de modifier un fichier auquel ils n'ont pas le droit d'accéder en écriture, le fichier est supprimé***.
- ***La suppression inopinée d'un périphérique peut entraîner la corruption du système de fichiers et des données du périphérique en question***.
- ***Si des utilisateurs tentent de copier des fichiers auxquels ils n'ont pas accès en écriture, ces fichiers sont temporairement visibles dans Windows Explorer ou d'autres applications de gestion de fichiers. En réalité, ces fichiers n'existent pas vraiment sur le périphérique cible, ils sont situés dans la mémoire cache et sont supprimés dès que DeviceLock a terminé d'en vérifier le contenu***.
- ***Lorsqu'un utilisateur ne disposant pas du droit d'accès en écriture à un contenu essaie d'insérer ce contenu dans un fichier qu'il a ouvert sur un périphérique USB, ledit fichier est supprimé lors de la tentative d'enregistrement***.
- ***La vérification du contenu des fichiers peut prendre du temps. Vous ne pourrez pas retirer le périphérique tant que cette opération est en cours, même si les fichiers copiés apparaissent dans Windows Explorer ou d'autres applications de gestion de fichiers. Dans ce cas, vous recevrez un message d'erreur indiquant que le périphérique est en cours d'utilisation***.
- ***Les fichiers récemment copiés ne peuvent pas être ouvert en lecture tant que DeviceLock n'a pas fini de vérifier leur contenu***.
- ***Le processus de vérification du contenu des fichiers peut prendre du temps. Vous pouvez définir un «Content verification message» à afficher aux utilisateurs lorsque la vérification de contenu est en cours. Pour obtenir des informations détaillées sur ce message, lire la section «***Message de vérification de contenu***» dans «Options de service.»***
- ***Si des utilisateurs tentent de lire ou d'écrire des fichiers auxquels ils n'ont accès ni en lecture ni en écriture, ils reçoivent un message à lecture ou écriture bloquée par DeviceLock Content-Aware, si l'option Content-Aware blocked read or write message est activée dans les Service Options. Pour obtenir des informations détaillées sur ces messages, lire les sections***

«**Message de lecture bloquée contextuel**» et «**Message d'écriture bloquée contextuel**» dans «Options de service.»

Règles contextuelles pour copies de réplication

Avant de pouvoir utiliser les règles contextuelles pour les copies de réplications, vous devez activer la réplication dans **Auditing and Shadowing** au niveau du type de périphérique. Les règles contextuelles qui s'appliquent aux copies de réplication filtrent les copies de réplication des fichiers écrits par l'utilisateur.

Le tableau suivant contient un résumé des droits de réplication susceptibles d'être indiqués dans les règles contextuelles.

DROITS DE REPLICATION	DESCRIPTION
Generic: Write	Contrôle la réplication ou non des contenus indiqués et enregistrés sur un périphérique. S'applique aux périphériques de types disquettes, iPhone, amovibles, Palm et Windows Mobile.
Generic: Print	Contrôle la réplication ou non des documents comportant les contenus indiqués et envoyés à des imprimantes. Ne s'applique qu'aux périphériques de type Imprimante. *DeviceLock extrait et analyse le texte des fichiers PostScript, PCL5, et PCL6*.
Encrypted: Write	Contrôle la réplication ou non des contenus indiqués et enregistrés sur un périphérique crypté. Ne s'applique qu'aux dispositifs de type amovibles.
Special Permissions: Write Calendar	Contrôle la réplication ou non des contenus indiqués et enregistrés sur un calendrier ou un périphérique mobile à partir d'un PC. S'applique aux périphériques de types iPhone, Palm et Windows Mobile.
Special Permissions: Write Contact	Contrôle la réplication ou non des contacts comportant les contenus indiqués et enregistrés sur un périphérique mobile à partir d'un PC. S'applique aux périphériques de types iPhone, Palm et Windows Mobile.
Special Permissions: Write E-mail	Contrôle la réplication ou non des courriels comportant les contenus indiqués et enregistrés sur un périphérique mobile à partir d'un PC. S'applique aux périphériques de types iPhone, Palm et Windows Mobile. Pour les iPhone, ce droit contrôle la réplication des paramètres de compte de messagerie mais pas des courriels eux-mêmes, car iTunes ne permet pas la synchronisation des messages.
Special Permissions: Write Attachment	Contrôle la réplication ou non des pièces jointes à des courriels, comportant les contenus indiqués et enregistrées sur un périphérique Windows Mobile ou Palm à partir d'un PC.
Special Permissions: Write Favorite	Contrôle la réplication ou non des favoris comportant les contenus indiqués et enregistrés sur un périphérique Windows Mobile ou un iPhone à partir d'un PC.
Special Permissions: Write File	Contrôle la réplication ou non des fichiers comportant les contenus indiqués et enregistrés sur un périphérique mobile à partir d'un PC. S'applique aux

DROITS DE REPLICATION	DESCRIPTION
	périphériques de types iPhone, Palm et Windows Mobile.
Special Permissions: Write Media	Contrôle la réplication ou non des données de supports comportant les contenus indiqués et enregistrées à l'aide de Windows Media Player sur un périphérique Windows Mobile à partir d'un PC, et des fichiers de supports comportant les contenus indiqués et enregistrés sur un périphérique Palm ou un iPhone à partir d'un PC.
Special Permissions: Write Backup	Contrôle la réplication ou non des données de sauvegarde comportant les contenus indiqués et enregistrées sur un iPhone à partir d'un PC.
Special Permissions: Write Note	Contrôle la réplication ou non des remarques comportant les contenus indiqués et enregistrées sur un périphérique mobile à partir d'un PC. S'applique aux périphériques de types iPhone, Palm et Windows Mobile.
Special Permissions: Write Pocket Access	Contrôle la réplication ou non des bases de données Pocket Access comportant les contenus indiqués et enregistrées sur un périphérique Windows Mobile à partir d'un PC.
Special Permissions: Write Task	Contrôle la réplication ou non des tâches comportant les contenus indiqués et enregistrées sur un périphérique mobile à partir d'un PC. S'applique aux périphériques de types Palm et Windows Mobile.
Special Permissions: Write Expense	Contrôle la réplication ou non des données d'applications Palm Expense comportant les contenus indiqués et enregistrées sur un périphérique Palm à partir d'un PC.
Special Permissions: Write Document	Contrôle la réplication ou non des documents Palm comportant les contenus indiqués et enregistrés sur un périphérique Palm à partir d'un PC.
Special Permissions: Write Unidentified Content	Contrôle la réplication ou non des autres données n'appartenant pas à l'une des catégories ci-dessus mais comportant les contenus indiqués et enregistrées sur un périphérique Windows Mobile à partir d'un PC.

Remarque: Les droits de réplication générique attribués aux périphériques de type Removable ne concernent que les périphériques non cryptés. Les droits de réplication cryptée attribués aux périphériques de type Removable ne concernent que les périphériques cryptés. Pour attribuer des droits de réplication à la fois aux périphériques Removable cryptés et non cryptés, vous devez attribuer des droits de réplication tant génériques que cryptés.

Configuration de paramètres de détection de contenu

Les règles contextuelles sont créées sur la base de groupes de contenus permettant de définir, de façon centralisée, les types de contenus pour lesquels vous désirez appliquer des restrictions d'accès. Les groupes de contenus indiquent le critère de filtrage à utiliser pour la sélection des données auxquelles les règles doivent s'appliquer.

Tous les groupes de contenus sont stockés dans la base de contenus. La même base de contenus est utilisée à la fois pour les périphériques et pour les protocoles. La base de contenus fait partie de la politique DeviceLockService et est également enregistrée dans un fichier XML, avec les paramètres de service que l'on peut créer à partir de DeviceLock

Management Console, de DeviceLock Service Settings Editor ou de DeviceLock Group Policy Manager.

Il existe plusieurs types de groupes de contenus: Les groupes File Type Detection, les groupes Keywords, les groupes Pattern, les groupes Document Properties et les groupes Complex. Ces différents groupes, ainsi que leur mode d'utilisation, sont décrits dans les sections ci-dessous.

Groupes File Type Detection Content

Les groupes File Type Detection servent à contrôler l'accès aux fichiers au niveau typologique. Ces groupes contiennent les définitions des types de fichiers qui les constituent. Une définition de type de fichier comporte deux propriétés: une extension de nom de fichier (par exemple, DOC) et une description (par exemple, document Microsoft Word). Lorsque vous définissez une règle basée sur un groupe File Type Detection, elle s'applique à tous les types de fichiers contenus dans ce groupe.

Définir des règles basées sur des groupes File Type Detection permet, par exemple, d'accorder l'accès en lecture aux documents Word à partir des disquettes à certains utilisateurs ou groupes d'utilisateurs, tout en leur refusant l'accès en écriture aux documents Word sur des disquettes. Vous pouvez refuser l'accès en lecture à tous les fichiers exécutables présents sur des périphériques amovibles, sur des CD/DVD et sur des disquettes, mais accorder l'accès en écriture à tous les types de fichiers présents sur des périphériques amovibles et des disquettes. Vous pouvez également spécifier que seuls des documents Word, Excel et PDF peuvent faire l'objet d'une copie de réplication.

DeviceLock comprend 34 groupes File Type Detection prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
Archives	MS Outlook & Outlook Express
Audio, Video & Flash	MS PowerPoint
BlackBerry	MS Project
Common Object File Format (COFF)	MS Publisher
Database	MS Visio
Executable	MS Windows Installer
Fax Documents	MS Windows Memory Dump
FileMaker Pro	MS Word
Fonts	MS Works
Help Files	OpenOffice, StarOffice, OpenDocument, etc.
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
Lotus SmartSuite	QuickBooks, Quicken, TurboTax & etc.
MS Access	Rich Text Format
MS Excel	Security Certificates

GROUPES DE CONTENUS INTEGRES	
MS InfoPath MS Money MS OneNote	Text, HTML & XML Virtual Machines WordPerfect Office

Remarque: Les règles contextuelles prennent en charge les formats Word To Go, Sheet To Go et Slideshow To Go des périphériques Palm. Le format Word To Go est inclus dans les groupes de contenus intégrés MS Word et Rich Text Format, le format Sheet To Go est inclus dans le groupe de contenus intégré MS Excel, alors que le format Slideshow To Go est inclus dans le groupe de contenus intégré MS PowerPoint.

Les fichiers Microsoft Word ou Rich Text Format (RTF), les fichiers Excel et les fichiers PowerPoint peuvent être transférés à un périphérique Palm à l'aide de l'application Documents To Go. L'application Documents To Go convertit ces fichiers dans des formats spéciaux: Les fichiers Word et RTF sont convertis au format Word To Go, les fichiers Excel sont convertis au format Sheet To Go, et les fichiers PowerPoint sont convertis au format Slideshow To Go. Les fichiers convertis sont automatiquement téléchargés sur le Palm lorsque les utilisateurs se synchronisent.

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les définitions de type de fichier contenues dans les groupes File Type Detection intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création de groupes de détection de types de fichiers personnalisés

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes de contenus de détection de types de fichiers personnalisés permettent de spécifier les types de fichiers que vous souhaitez inclure dans le même groupe afin de mieux répondre aux besoins particuliers de votre entreprise.

Supposez par exemple que vous deviez autoriser certains utilisateurs à accéder aux documents Word, Excel et PDF, ainsi qu'aux fichiers graphiques. Pour ce faire, commencez par créer un nouveau groupe de contenus comportant ces types de contenus. Puis, définissez une règle en fonction du groupe de contenus ainsi personnalisé.

Pour créer un groupe de détection de types de fichiers personnalisés

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

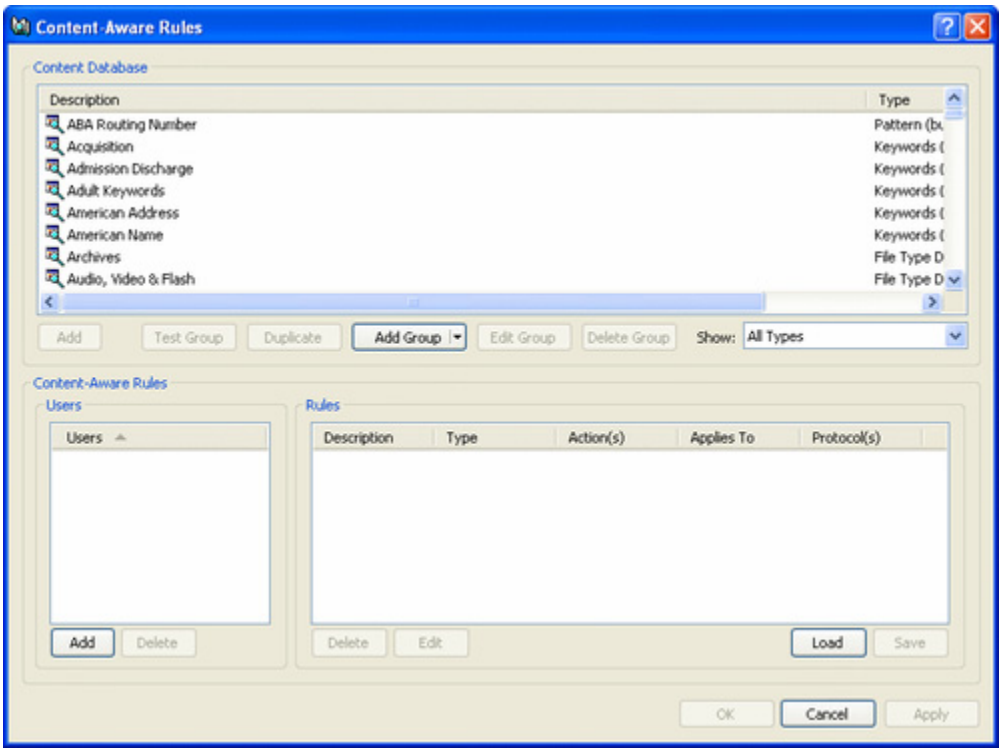
   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

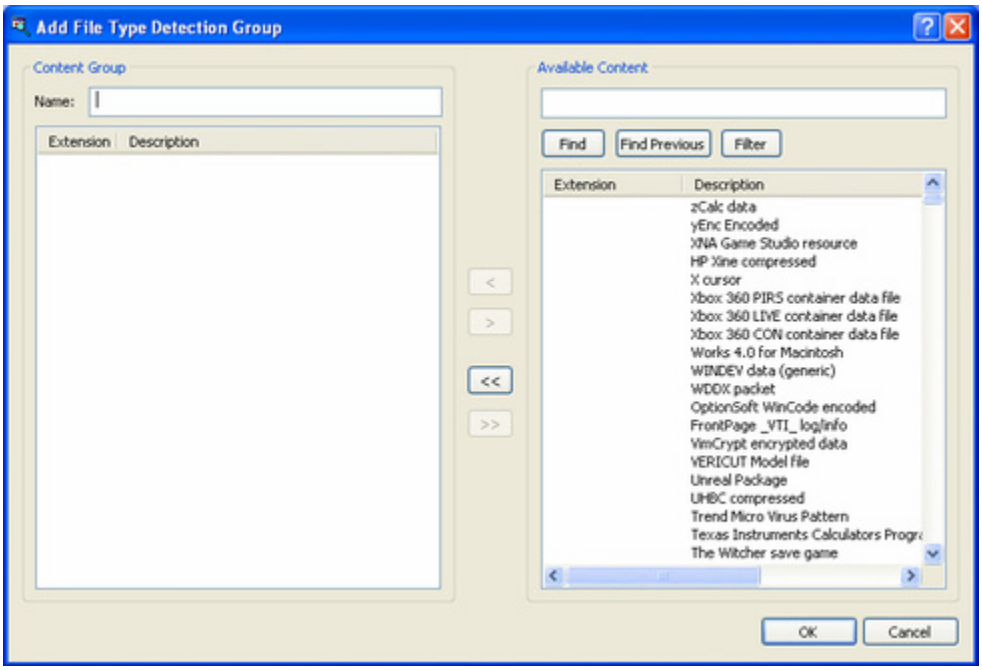
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **File Type Detection**.

La boîte de dialogue Add File Type Detection Group apparaît.



5. Dans le panneau de gauche de la boîte de dialogue **Add File Type Detection Group**, sous **Content group**, saisissez le nom du nouveau groupe de contenus dans la boîte **Name**.
6. Dans le panneau de droite de la boîte de dialogue **Add File Type Detection Group**, sous **Available Content**, sélectionnez tous les types de fichiers que vous souhaitez ajouter au nouveau groupe de contenus, puis cliquez sur le bouton comportant une flèche simple orientée vers la gauche [<].

   Pour sélectionner plusieurs types de fichiers, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

   Pour supprimer des types de fichiers individuels du groupe de contenus, utilisez le bouton comportant une flèche simple orientée vers la droite [>]. Pour ajouter ou supprimer d'un seul coup tous les types de fichiers disponibles dans le groupe de contenus, utilisez le bouton comportant une flèche double orientée vers la gauche [<<] ou vers la droite [>>].

   Remarque: Vous pouvez rechercher les types de fichiers disponibles dans la base de contenus par extension ou par description. Vous pouvez utiliser des caractères génériques comme les astérisques (*) et les points d'interrogation (?) pour rechercher un groupe ou des types de fichiers donnés. Pour trouver un type ou un groupe de types de fichiers donné, dans **Available Content**, saisissez une extension ou une description avec ou sans caractères génériques dans la séquence de recherche, puis cliquez sur **Find**. Pour filtrer les types de fichiers, cliquez sur **Filter**. Pour supprimer le filtre, appliquez-le à une séquence vide.

   L'astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser ces caractères génériques n'importe où et en nombre illimité.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Add File Type Detection Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la

boîte de dialogue Content-Aware Rules.

Groupes de contenus Keywords

Les groupes Keywords permettent de contrôler l'accès aux fichiers en fonction de l'occurrence de certains mots dans un document.

Des règles à base de groupes de mots clés permettent, par exemple, d'accorder l'accès en lecture à tous les documents contenant les expressions «Top secret» et «Pour utilisation officielle uniquement» présents sur des périphériques amovibles, des disquettes et des DVD/CD-ROM, tout en refusant l'accès en écriture aux périphériques amovibles et aux disquettes pour les mêmes documents. Vous pouvez aussi spécifier que seuls les documents contenant les expressions «Top secret» et «Pour utilisation officielle uniquement» peuvent faire l'objet d'opérations de copie de réplication.

DeviceLock comprend 157 groupes Keywords prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss
Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property
American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation
Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital

GROUPES DE CONTENUS INTEGRES

Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses
Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver's License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medicinal Active Substances
FITS Date & Time	Russian: Medicinal Drugs
FITS File Checksum	Russian: Noncompliant
FITS File Descriptors	Russian: Passwords and Access Codes
FITS Hierarchical file grouping	Russian: Physical Security
FITS Instrumentorum	Russian: Prices
FITS Non-standard	Russian: Project Documentation
FITS Observations	Russian: Project Names
FITS Standard	Russian: Project Versions
Gambling	Russian: Projects Release Date
Grades	Russian: Technology
HCFA (CMS) 1500 Form	Russian: User Names
HIPAA - Diseases	Russian: Working Conditions
HIPAA HCPCS	Sales Forecast
HIPAA ICD9	Sarbanes-Oxley Sensitive
HIPAA NDC Classes	Security
HIPAA NDC Dosages	Security Agencies
HIPAA NDC Listing	Sensitive Disease
HIPAA NDC Routes	Sexual Language
Illegal Drugs	Social Security
Innovations	SPAM
Internet Slang Abbreviations	Sports
Investments	Staff Training
Java Source Code	Substance Abuse
Market Development	Suspicious Activity Report
Medical Diagnosis	Technology
Medical Record Numbers	UBO4 Form
MEMO	US Birth Date
Network Security	US Birth Place
Partner Names	US Expiry Date
Password	User Name
Payments	VB Source Code
PCI GLBA	Violence
Perl Source Code	Weapon Keywords
Price List	Wire Transfer
Prices	Working Conditions
Pro Earnings	

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les mots clés contenus dans les groupes Keywords intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création d'un groupe Keywords personnalisé

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes de contenus Keywords personnalisés permettent de spécifier les mots clés que vous souhaitez inclure dans le même groupe afin de mieux répondre aux besoins particuliers de votre entreprise.

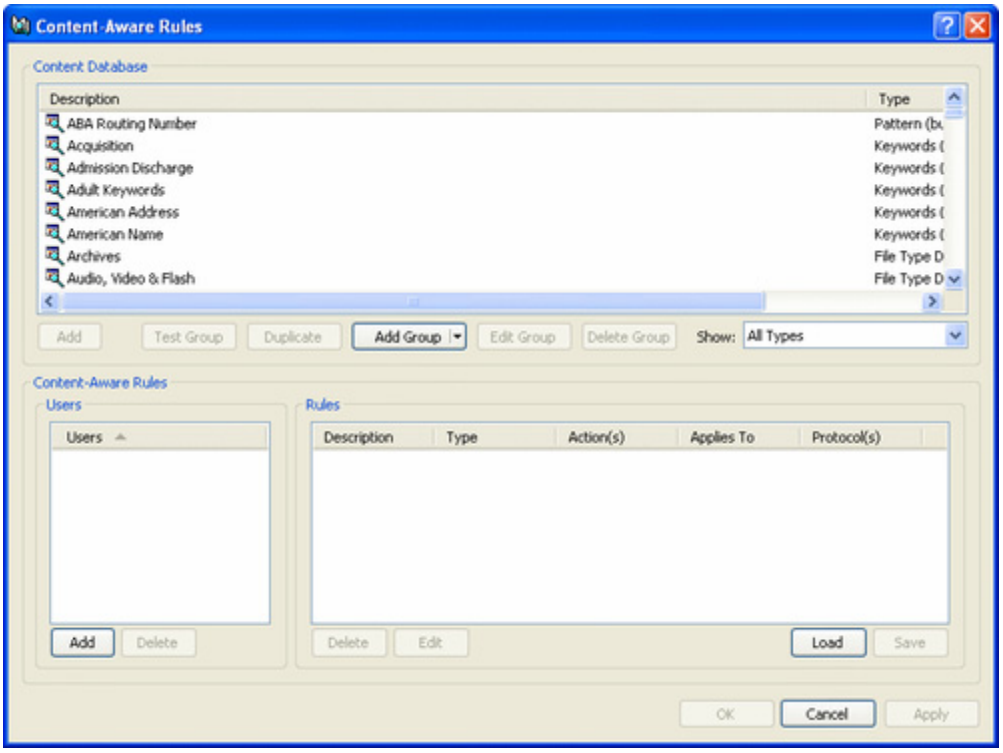
Pour créer un groupe Keyword personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

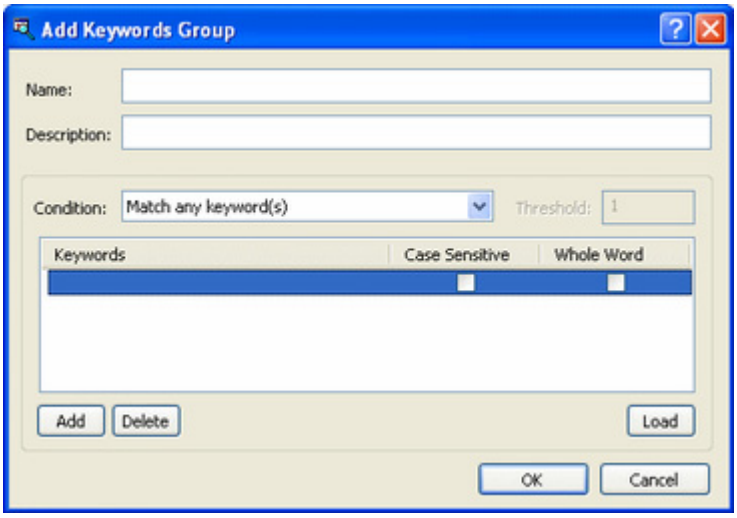
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Keywords**.

   La boîte de dialogue Add Keywords Group apparaît.



5. Dans la boîte de dialogue **Add Keywords Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Description:	Donner une description pour le groupe.
Condition:	Préciser les conditions d'application des règles associées à ce groupe de contenu. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Condition:** • **Match any keyword(s)** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que l'un des mots clés spécifiés figure dans les données de texte. • **Match all keyword(s)** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que tous les mots clés spécifiés figurent dans les données de texte. • **Only when combined score exceeds (or equal to) threshold** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre total (la somme) des occurrences de tous les mots clés figurant dans les données de texte égale ou dépasse le nombre maximum d'occurrences des mots clés.
Threshold	Indiquer un nombre maximum d'occurrences des mots clés. Ce nombre peut varier entre 0 et 65535. Ce paramètre doit être renseigné si vous avez sélectionné l'option **Only when combined score exceeds (or equal to) threshold**.
Keywords	Indiquer les mots ou les expressions à rechercher dans le texte des données. Double-cliquez sur **Keywords** pour saisir un mot clé ou une expression.
Case Sensitive	Préciser la sensibilité à la casse des mots clés. Cochez la case **Case Sensitive** pour activer la sensibilité à la casse (à titre d'exemple, les mots «test» et «Test» seront considérés comme étant des mots clés différents). Décochez la case **Case Sensitive** pour désactiver la sensibilité à la casse (à titre d'exemple, les mots «test» et «Test» seront considérés comme étant un même mot clé).
Whole Word	Indiquer les options de correspondance du mot clé. Cochez la case **Whole Word** pour activer l'option de correspondance exacte (permet de rechercher une correspondance exacte du mot clé). Décochez la case **Whole Word** pour désactiver l'option de correspondance exacte (permet de rechercher des variantes grammaticales du mot clé).
Weight	Indiquer le degré d'importance de chaque mot clé ou expression. Le paramètre Weight sert à compter le nombre d'occurrences des mots clés spécifiés dans le texte des données. Ce paramètre doit être renseigné si vous avez sélectionné l'option **Only when combined score exceeds (or equal to) threshold**. Valeurs possibles: **Heavy**, **Above Normal**, **Normal** (valeur par défaut), **Below Normal**, **Light**. Ces valeurs du paramètre Weight peuvent être interprétées de la manière suivante: **Heavy**: indique que chaque occurrence est comptabilisée trois fois. C'est la valeur la plus élevée. **Above Normal**: indique que chaque occurrence est comptabilisée deux

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
	fois. **Normal**: indique que chaque occurrence est comptabilisée une fois. **Below Normal**: indique que deux occurrences comptent pour une. **Light**: indique que trois occurrences comptent pour une. C'est la valeur la plus faible.
Add	Indiquer les mots clés et les expressions clés. Cliquez sur **Add** pour entrer un mot clé ou une expression clé.
Delete	Supprimer un mot clé. Pour ce faire, sélectionnez le mot clé que vous souhaitez supprimer et cliquez sur **Delete**. Pour sélectionner plusieurs mots clés, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
Load	Importer une liste de mots clés à partir d'un fichier TXT.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Keywords Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes de contenus Pattern

Les groupes de contenus Pattern permettent de contrôler l'accès à des fichiers texte en utilisant des modèles de texte décrits par des expressions régulières Perl. Ces modèles fournissent un moyen, flexible et efficace, de détection automatique des contenus sensibles (par exemple, numéros de cartes de crédit, numéros de sécurité sociale, adresses email et numéros de téléphone) dans les documents.

Pour plus d'informations sur la création et l'utilisation des expressions régulières Perl, veuillez consulter le Tutoriel rapide sur les expressions régulières Perl et le Tutoriel sur les expressions régulières Perl (en anglais).

Les règles basées sur les groupes Pattern permettent, par exemple, de refuser à certains utilisateurs ou groupes d'utilisateurs l'accès en écriture aux documents contenant des numéros de cartes crédit sur les périphériques amovibles et les disquettes. Vous pouvez également désactiver la copie de réplication des documents ne contenant pas de numéro de carte de crédit.

DeviceLock comprend 45 groupes Pattern prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
ABA Routing Number BIC (ISO 9362) Canadian Social Insurance Number Credit Card Number Email Address European VAT Number GPS Data (RMC String) IBAN International Telephone Number IP Address ISO Date MAC Address Microsoft Windows Product Key Russian: Address Russian: Auto Insurance Number Russian: Bank Account Number Russian: BIC Russian: Car Numbers Russian: Classification of Economic Activities Russian: Classification of Enterprises and Organizations Russian: Driver's License Number Russian: Health Insurance Number Russian: International Passport	Russian: Main State Registration Number Russian: Motorcycle Numbers Russian: Passport Russian: Pension Insurance Number Russian: Post Code Russian: Taxpayer Identification Number Russian: Telephone Number Russian: Trailer Numbers Russian: Vehicle Registration Document SQL Queries TCP/UDP Port Number Time (12/24h) UK National Insurance Number UK Phone Number UK Post Code UK Tax Code Uniform Resource Locator (URL) US Date US Phone Number US Social Security Number US Zip Code VIN

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les modèles d'expressions régulières contenus dans les groupes Pattern intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création d'un groupe Pattern personnalisé

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes de contenus personnalisés permettent de préciser le modèle que vous souhaitez utiliser pour identifier des informations sensibles dans les documents.

Pour créer un groupe Pattern personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

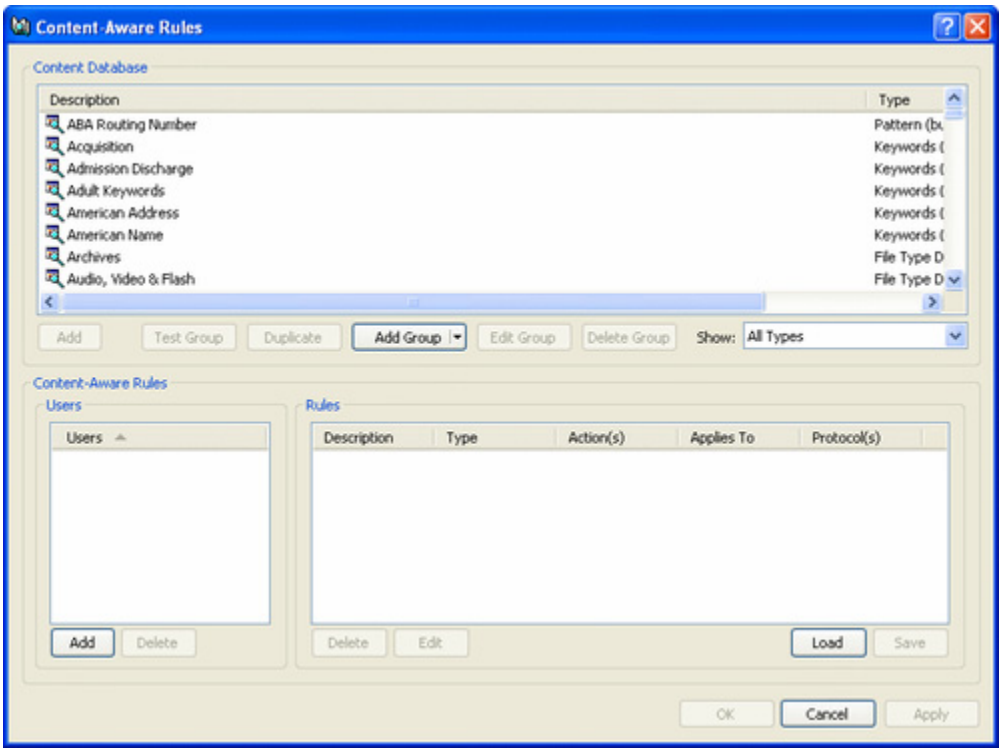
   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

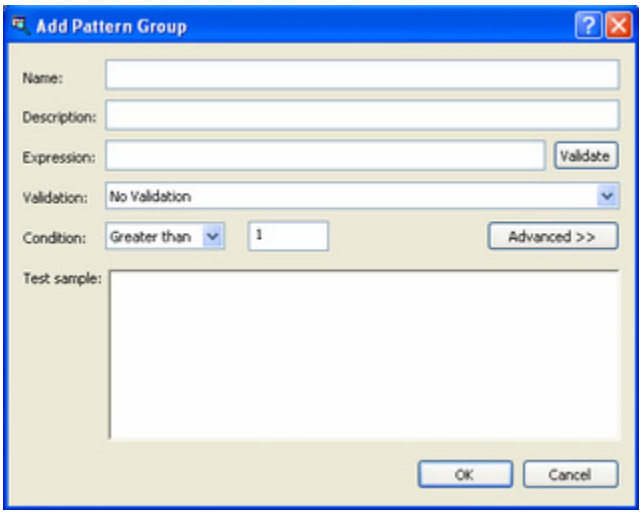
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Pattern**.

   La boîte de dialogue Add Pattern Group apparaît.



5. Dans la boîte de dialogue **Add Pattern Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
Expression	Indiquer le modèle en créant une expression régulière. Pour plus d'informations sur la création des expressions régulières Perl, veuillez consulter le Tutoriel rapide sur les expressions régulières Perl et le Tutoriel sur les expressions régulières Perl (en anglais).
Validate	Vérifier la syntaxe de l'expression régulière.
Validation	Effectuer la validation réelle des correspondances potentielles renvoyées par l'expression régulière. Les options suivantes sont disponibles: **No validation** (Cette option est sélectionnée par défaut.), **ABA Routing Number**, **Canadian Social Insurance Number**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Date, Date (ISO)**, **Email Address**, **European VAT Number**, **IBAN**, **IP Address**, **LUHN Checksum**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations**, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social Security Number**.
Condition:	Préciser les conditions d'application des règles associées à ce groupe de contenu. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Condition**: • **Less than or =** indique qu'une règle associée à ce groupe de

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
	contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est inférieur ou égal au nombre spécifié. • **Equal to** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est égal au nombre spécifié. • **Greater than or =** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est supérieur ou égal au nombre spécifié. • **Between** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière se trouve dans la plage spécifiée.
Advanced	Effectuer un test rapide du modèle de l'expression régulière sur des données-échantillon. Cliquez sur **Advanced** pour afficher ou masquer la boîte **Test sample**.
Test sample	Entrer une chaîne à tester et voir le résultat. DeviceLock prend en charge la mise en surbrillance de couleur en temps réel des résultats. Tous les résultats concordants sont surlignés en vert, tandis que les chaînes qui ne correspondent pas au modèle sont surlignées en rouge.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Pattern Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes de contenus Document Properties

Les groupes Document Properties permettent de contrôler l'accès aux fichiers en fonction des propriétés des fichiers telles que le nom, la taille du fichier... Ils permettent également de contrôler l'accès aux documents et aux archives protégés par mot de passe, ainsi qu'aux images textes.

Remarque: Le ET logique s'applique à toutes les propriétés des fichiers contenus dans un groupe Document Properties. À titre d'exemple, si vous voulez contrôler l'accès aux fichiers de plus de 5 mégaoctets (Mo) et aux documents et archives protégés par mot de passe, vous devez créer deux groupes Document Properties distincts : un groupe pour le contrôle d'accès aux fichiers de plus de 5 Mo et un groupe pour le contrôle d'accès aux documents et aux archives protégés par mot de passe. Si vous spécifiez ces propriétés de fichiers dans le même groupe Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera les documents et les archives protégés par mot de passe dont la taille est supérieure à 5 Mo.

Les règles basées sur les groupes Document Properties permettent, par exemple, d'accorder l'accès en lecture à tous les documents de plus d'1 Mo sur des périphériques amovibles, des disquettes et DVD/CD-ROM, tout en refusant l'accès en écriture sur ces mêmes

périphériques pour les mêmes documents. Vous pouvez également spécifier que seuls les documents dont la taille excède 5 Mo peuvent faire l'objet d'une copie de réplication.

DeviceLock n'intègre pas de groupe de contenus Document Properties prédéfinis. La procédure suivante indique comment créer un groupe Document Properties.

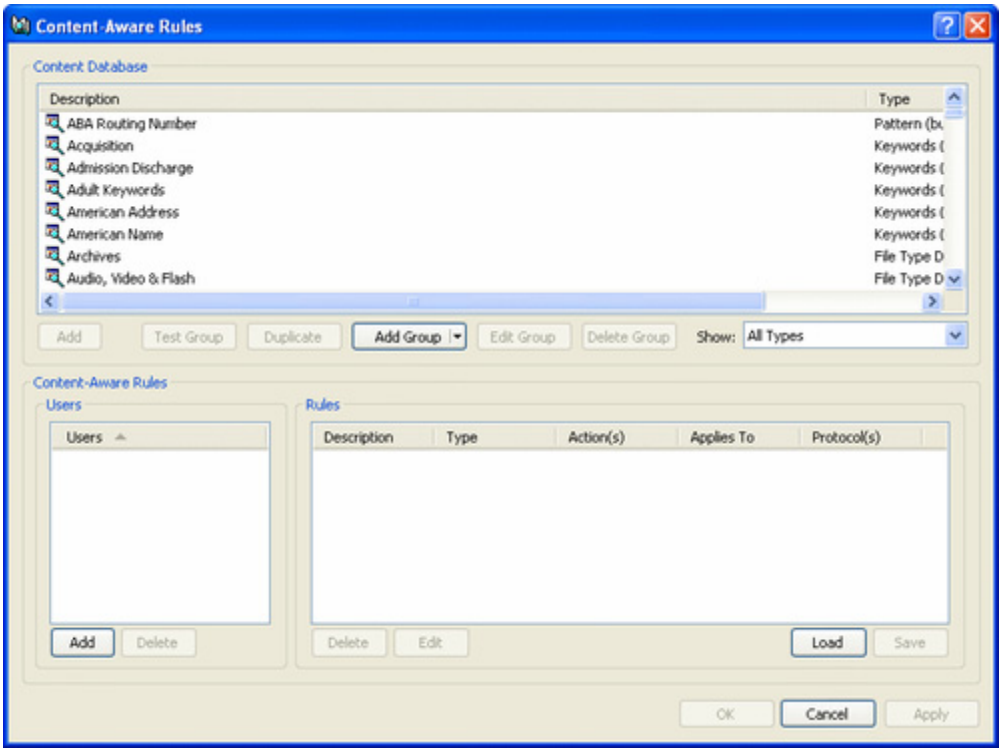
Pour créer un groupe Document Properties

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

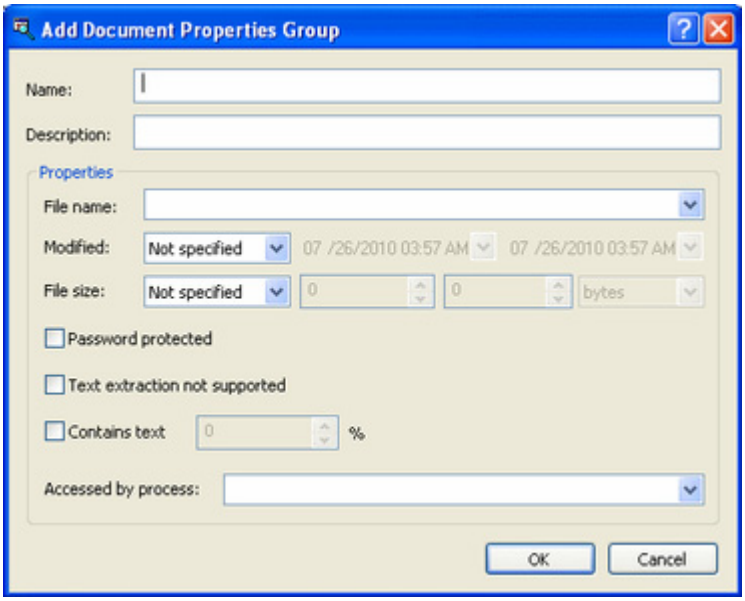
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Document Properties**.

   La boîte de dialogue Add Document Properties Group apparaît.



5. Dans la boîte de dialogue **Add Document Properties Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
File name	Indiquer le nom des fichiers. Vous pouvez utiliser des jokers comme les astérisques (*) et les points d'interrogation (?). Par exemple, saisissez ***.txt** pour indiquer tous les fichiers avec l'extension .txt Les différents noms de fichiers doivent être séparés par un point-virgule (;), par exemple: ***.doc; *.docx**. *L'astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple*. **Remarque :** Pour la réplication des données capturées à partir du périphérique imprimante, la valeur du nom de fichier que vous spécifiez est comparée avec les noms fournis dans la colonne **File Name** du Shadow Log Viewer.
Modified	Indiquer la dernière date et heure de modification du fichier. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Modified**: • **Not specified** (cette option est sélectionnée par défaut). • **Before than**: indique que la date et l'heure de modification du fichier doivent être antérieures à la date et à l'heure indiquées. • **After than**: indique que la date et l'heure de modification du fichier doivent être ultérieures à la date et à l'heure indiquées. • **Between**: indique que la date et l'heure de modification du fichier doivent être comprises dans la plage indiquée. • **Not older than**: indique que la date et l'heure de modification du fichier ne doivent pas être plus grands que le nombre de secondes, minutes, jours, semaines, mois et années indiqué. • **Older than**: indique que la date et l'heure de modification du fichier doivent être plus grands que le nombre de secondes, minutes, jours, semaines, mois et années indiqué.
File size	Indiquer la taille du fichier en octets, kilo-octets, méga-octets, giga-octets ou téra-octets. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **File size**: • **Not specified** (cette option est sélectionnée par défaut). • **Equal to**: indique que les fichiers doivent être d'une taille égale à la taille indiquée. • **Less than**: indique que les fichiers doivent être d'une taille inférieure à la taille indiquée. • **More than**: indique que les fichiers doivent être d'une taille supérieure à la taille indiquée. • **Between**: indique que la taille des fichiers doit se situer dans la plage indiquée.
Password protected	Détecter et contrôler l'accès aux archives, fichiers PDF et documents Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx) protégés par mot de passe. Si vous cochez la case **Password protected** pour un groupe

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
	Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera l'accès aux archives, fichiers PDF et documents Microsoft Office protégés par mot de passe. Décochez la case **Password protected** si vous ne souhaitez pas détecter et contrôler l'accès aux archives, fichiers PDF et documents Microsoft Office protégés par mot de passe. Pour plus d'informations sur les formats d'archives pris en charge, veuillez lire la description de la fonction «Vérification des fichiers contenus dans les archives.»
Text extraction not supported	Contrôler l'accès aux formats de fichiers non pris en charge. Si vous cochez la case **Text extraction not supported** pour un groupe Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera l'accès à tous les fichiers à format non pris en charge. Tous les formats pris en charge sont énumérés dans la section «Extension des fonctionnalités de DeviceLock avec ContentLock et NetworkLock.»
Contains text	Détecter et contrôler l'accès aux images selon qu'elles contiennent ou non du texte. Si vous cochez la case **Contains text** pour un groupe Document Properties, puis créez une règle contextuelle basée sur la combinaison de ce groupe de contenus et du groupe de contenus d'images intégrées et de dessins et autres fichiers CAD par l'opérateur logique AND, cette règle vérifiera si les images prises en charge contiennent du texte et contrôlera l'accès aux images contenant du texte. Décochez la case **Contains text** si vous ne souhaitez pas détecter et contrôler l'accès aux images contenant du texte. Pour plus d'informations sur les formats d'images pris en charge, veuillez lire la description de la fonction «Détection de texte dans les images.» Vous devez préciser la quantité de texte que les images doivent contenir si vous cochez la case **Contains text**. La quantité de texte est exprimée en pourcentage de la superficie totale de l'image. Par exemple, si le texte occupe la moitié de l'image, la quantité de texte sera 50 %. Si une image n'est constituée que de texte (document scanné par exemple), la quantité de texte est de 100 %. **Remarque:** L'option **Contains text %** s'applique également aux autres formats de fichiers pris en charge. Dans ce cas, le pourcentage est le rapport entre la taille du texte en caractères et la taille du fichier en octets.
Accessed by process	Indiquer le nom du processus en train d'accéder au fichier du document. Vous pouvez utiliser des jokers comme les astérisques (*) et les points d'interrogation (?). Les différents noms de processus doivent être séparés par un point-virgule (;), par exemple: **explorer.exe; notepad.exe**.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Document Properties Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes à contenus complexes

Les groupes à contenus complexes utilisent des expressions booléennes pour sélectionner les documents pour lesquels vous désirez contrôler l'accès. Ces groupes peuvent inclure toute combinaison de groupes de contenus intégrés ou personnalisés (groupes File Type Detection, Keywords, Pattern et Document Properties) connectés par un nombre quelconque d'opérateurs logiques. Chaque groupe de contenus est considéré comme un critère de filtre unique que vous pouvez inclure dans l'expression booléenne. L'utilisation de plusieurs groupes de contenus permet de créer des filtres complexes pour l'identification du contenu des documents sensibles.

Le tableau suivant répertorie les opérateurs logiques dans l'ordre de priorité décroissant.

OPERATEUR	SIGNIFICATION
NOT	Négation logique d'un critère de filtre
AND	Application simultanée des deux filtres
OR	Application de l'un ou l'autre critère de filtre

Vous pouvez utiliser des parenthèses pour modifier la priorité des opérateurs et forcer l'évaluation de certaines parties de l'expression avant les autres. Les critères imbriqués dans des parenthèses sont évalués de l'intérieur vers l'extérieur. DeviceLock prend en charge l'imbrication à plusieurs niveaux des critères. Un groupe complexe peut contenir au maximum 30 groupes de contenus.

DeviceLock n'intègre pas de groupe de contenus complexes prédéfinis. La procédure suivante indique comment créer un groupe complexe.

Pour créer un groupe complexe

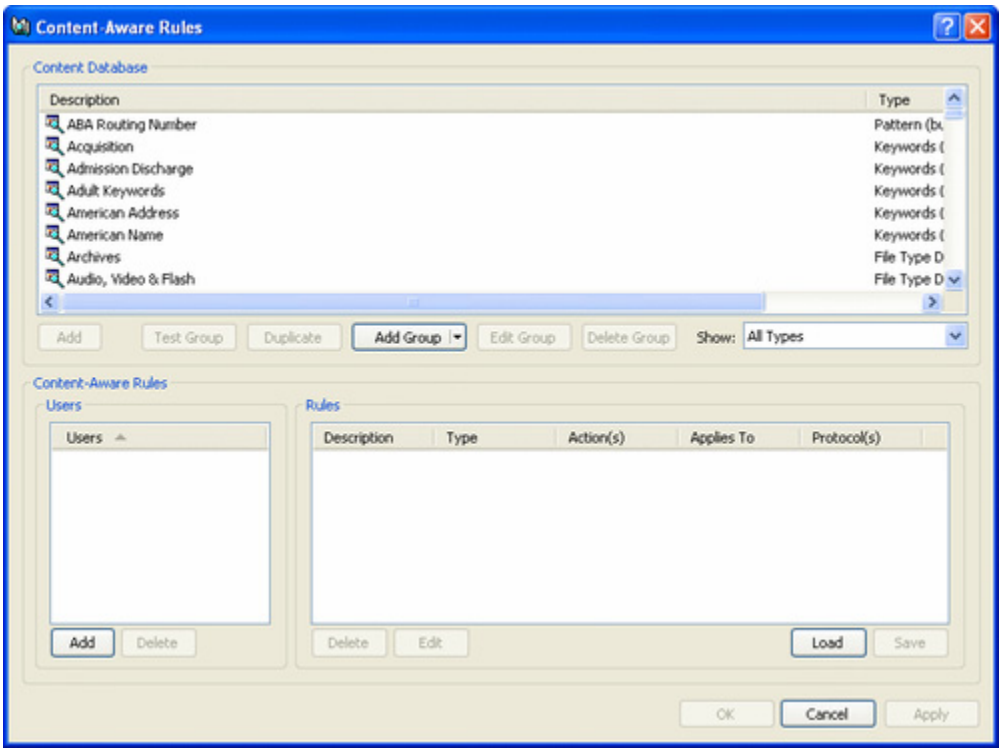
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
    a) Ouvrez Group Policy Object Editor.
    b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
    - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
    - OU -

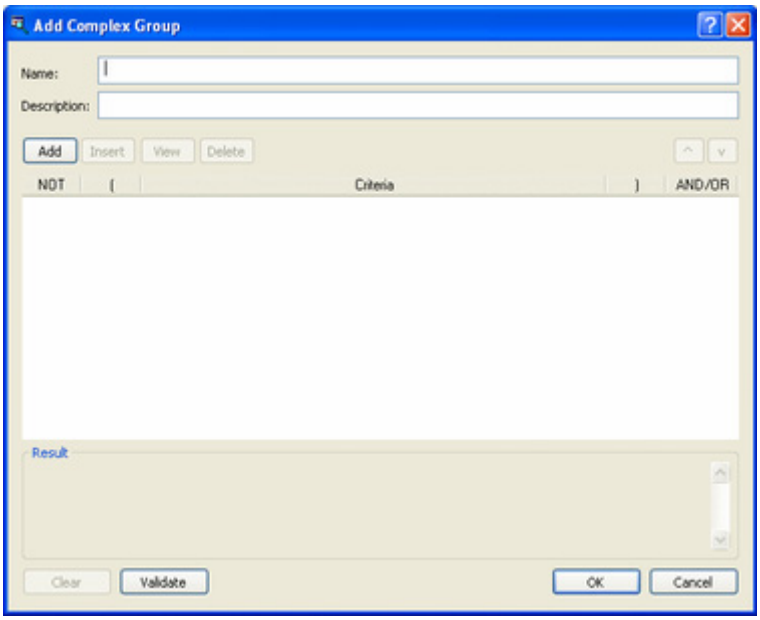
- Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Complex**.

   La boîte de dialogue Add Complex Group apparaît.



5. Dans la boîte de dialogue **Add Complex Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
Add	Ajouter des groupes de contenus à partir de la base de contenus. Pour ce faire, cliquez sur **Add** pour ouvrir la boîte de dialogue **Content Groups**. Dans le champ **Content Database** de la boîte de dialogue **Content Groups**, sélectionnez le groupe désiré et cliquez sur **OK**. *Pour sélectionner plusieurs groupes de contenus, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. *Pour voir les informations concernant un groupe de contenus, sélectionnez le groupe concerné et cliquez sur View Group*. *Les groupes de contenus que vous avez ajoutés apparaissent dans la colonne Criteria de la boîte de dialogue Add Complex Group. Chaque groupe de contenus que vous ajoutez est considéré comme un critère de filtre unique que vous pouvez inclure dans l'expression booléenne*.
Insert	Insérer un groupe de contenus, avant le groupe actuellement sélectionné dans la colonne **Criteria**, à partir de la base de contenus. Pour ce faire, cliquez sur Insert pour ouvrir la boîte de dialogue **Content Groups**. Dans le champ **Content Database** de la boîte de dialogue **Content Groups**, sélectionnez le groupe désiré et cliquez sur **OK**.
View	Voir les informations concernant le groupe actuellement sélectionné dans la colonne **Criteria**.
Delete	Supprimer le groupe sélectionné de la colonne **Criteria**.
NOT	Appliquer l'opérateur logique NOT à chaque groupe sélectionné. Pour ce faire, sélectionnez le groupe de votre choix dans la colonne **Criteria** et cochez la case appropriée dans la colonne **Not**.
AND/OR	Appliquer l'opérateur logique AND ou l'opérateur logique OR à chaque groupe sélectionné. Pour ce faire, sélectionnez le groupe de votre choix dans colonne **Criteria** et cochez la case appropriée dans la colonne **AND/OR**.
Clear	Effacer la liste de groupes de contenus actuelle dans la colonne **Criteria**.
Validate	Valider votre expression. Si l'expression n'a pas été définie proprement (il existe par exemple une parenthèse ouvrant ne correspondant à aucune parenthèse fermante), un message d'erreur s'affichera.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Complex Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Consulter les groupes de contenus intégrés

Vous pouvez consulter tous les groupes de contenus intégrés, mais vous ne pouvez ni les modifier ni les supprimer.

Pour voir un groupe de contenus intégré

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
    a) Ouvrez Group Policy Object Editor.
    b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
    - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
      - OU -
    - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

    La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez un groupe de contenus intégré que vous souhaitez consulter, puis cliquez sur **View Group**.

Dupliquer les groupes de contenus intégrés

Vous ne pouvez pas modifier les groupes de contenus intégrés. Toutefois, vous pouvez en créer des copies éditables (duplications), pour répondre aux besoins particuliers de votre entreprise.

Pour dupliquer un groupe de contenus intégré

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus que vous souhaitez dupliquer, puis cliquez sur **Duplicate**.
5. Dans la boîte de dialogue qui s'ouvre alors, effectuez les changements nécessaires, puis cliquez sur **OK**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Modification et suppression d'un groupe de contenus personnalisé

Vous pouvez à tout moment modifier ou supprimer des groupes de contenus personnalisés.

Pour modifier ou supprimer un groupe de contenus personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.

4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus personnalisé que vous souhaitez modifier ou supprimer.
5. Cliquez sur **Edit Group** pour modifier le groupe de contenu sélectionné. Dans la boîte de dialogue qui s'ouvre alors, effectuez les changements nécessaires puis cliquez sur **OK**.

   - OU -

   Cliquez sur **Delete Group** ou appuyez sur la touche DELETE (Suppr) pour supprimer le groupe de contenus sélectionné.
6. Dans la boîte de dialogue **Content-Aware Rules**, cliquez sur **OK** ou sur **Apply** pour appliquer les modifications.

Test des groupes de contenus

Vous pouvez tester n'importe quel groupe de contenus intégré ou personnalisé pour vérifier si les fichiers spécifiés y correspondent effectivement. Ces tests permettent de vérifier si les règles contextuelles créées sur la base de ces groupes répondent aux exigences particulières de votre entreprise.

Pour tester un groupe de contenus

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus que vous souhaitez tester, puis cliquez sur **Test Group**.

   Vous ne pouvez tester qu'un seul groupe de contenus à la fois.

   La boîte de dialogue Open apparaît.

5. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez utiliser pour tester le groupe de contenus spécifié.
6. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
7. Cliquez sur le fichier, puis sur **Open**.

   La boîte de message des résultats s'affiche. Si le fichier concorde avec le groupe de contenus indiqué, la boîte de message des résultats affichera le texte suivant: «Selected file matches with the group.» Si le fichier ne concorde pas avec le groupe de contenus indiqué, la boîte de message des résultats affichera le texte suivant: «Selected file does not match with the group.»

   Lorsque le test est en cours, la console ne répond plus (elle se bloque).

Gestion des règles contextuelles

La gestion des règles contextuelles comprend les tâches suivantes:

- Définition de règles contextuelles
- Modification de règles contextuelles
- Copie de règles contextuelles
- Exportation et importation de règles contextuelles
- Révocation de règles contextuelles
- Suppression de règles contextuelles

Les règles contextuelles peuvent être créées à l'aide de DeviceLock Management Console, de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor.

Définition de règles contextuelles

Les règles contextuelles sont créées sur la base des groupes de contenus intégrés ou sur la base des groupes de contenus personnalisés. Pour plus d'informations sur ces groupes, voir «Configuration des paramètres de détection de contenu.»

Pour définir une règle contextuelle

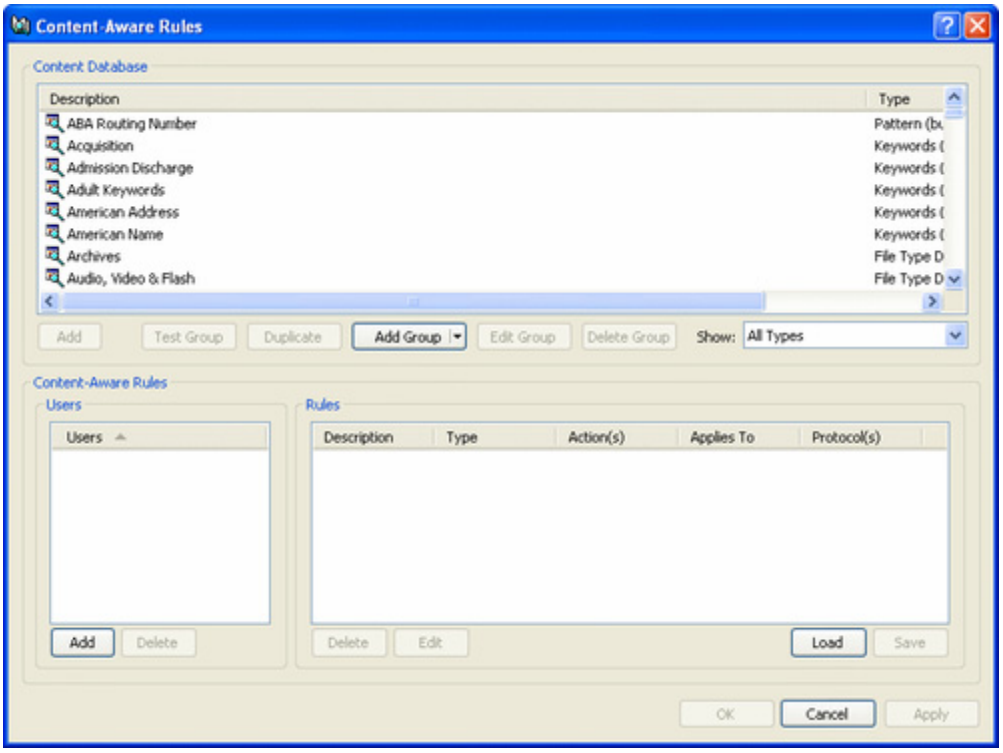
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez Computer Configuration, puis DeviceLock.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans la boîte de dialogue **Select Users or Groups**, champ **Enter the object names to select**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous avez ajoutés s'affichent sous Users dans le panneau inférieur gauche de la boîte de dialogue Content-Aware Rules.

   Pour supprimer un utilisateur ou un groupe, dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur et le groupe, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

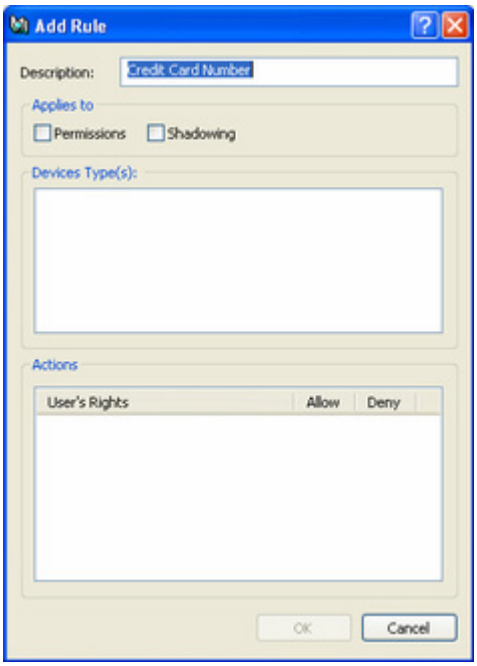
6. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez les utilisateurs ou les groupes pour lesquels vous souhaitez définir la règle.

Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sous **Content Database**, sélectionnez le groupe de contenus souhaité, puis cliquez sur Add.

   Remarque: Vous ne pouvez indiquer qu'un seul groupe de contenus par règle contextuelle.

   La boîte de dialogue Add Rule apparaît.



8. Dans la boîte de dialogue **Add Rule**, champ **Description**, saisissez le nom de la Content-Aware Rule.

   Par défaut, la Content-Aware Rule a le même nom que le groupe de contenus indiqué mais vous pouvez saisir un nom différent.

9. Sous **Applies to**, indiquez le type d'opération associé à la règle. Les options disponibles sont les suivantes:
   - **Permissions**: Indique que la règle s'appliquera aux opérations de contrôle d'accès.
   - **Shadowing**: Indique que la règle s'appliquera aux opérations de copie de réplication.
   - **Permissions**, **Shadowing**: Indique que la règle s'appliquera aux opérations de contrôle d'accès et de copie de réplication.

10. Dans **Device Type(s)**, sélectionnez le ou les types de périphériques auxquels vous souhaitez que cette règle s'applique.

    Les règles contextuelles peuvent être appliquées aux périphériques de types DVD/CD-ROM, Floppy, iPhone, Palm, Removable et Windows Mobile.

Si plusieurs types de périphériques sont sélectionnés dans le paramètre Action(s), la boîte de dialogue affichera uniquement les droits d'accès qui sont communs à tous les types de périphériques sélectionnés.

11. Dans **Action(s)**, indiquez les actions utilisateur qui sont autorisées ou non sur les fichiers, et celles qui sont consignées dans le journal de réplication.

    Vous pouvez sélectionner l'une ou l'autre des options suivantes: Read, Write, Read and Write.

    Si la règle s'applique aux copies de réplication ou à la fois au contrôle d'accès et aux copies de réplication, l'option Read devient disponible. Pour en savoir plus sur les droits d'utilisateur susceptibles d'être indiqués dans les règles contextuelles, consultez les chapitres intitulés «Règles contextuelles pour opérations de contrôle d'accès» et «Règles contextuelles pour copies de réplication.»

12. Cliquez sur **OK**.

    La règle ainsi créée est affichée dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules.

13. Cliquez sur **OK** ou **Apply** pour appliquer la règle.

    Les utilisateurs ou les groupes auxquels s'applique la Content-Aware Rule s'affichent dans la section Content-Aware Rules de l'arborescence. Si vous sélectionnez un utilisateur ou un groupe auquel la Content-Aware Rule s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

    - **Description** Le nom de la règle. Par défaut, la règle a le même nom que le groupe de contenus indiqué.
    - **Type** Le type de l'analyse de contenus. Valeurs possibles: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, et **Complex**. **File Type Detection** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs signatures propres. **Keywords** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des mots clés et des expressions spécifiés. **Pattern** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des modèles de textes décrits par les expressions régulières Perl. **Document Properties** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs propriétés. **Complex** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction du contenu décrit par une expression booléenne.
    - **Action(s)** Indique les actions utilisateur qui sont autorisées ou non sur les fichiers, et celles qui sont consignées dans le journal de réplication.
    - **Applies To** Valeurs possibles: **Permissions**, **Shadowing**, et **Permissions, Shadowing**. **Permissions** indique que la règle s'applique aux contrôles d'accès. **Shadowing** indique que la règle s'applique aux copies de réplication. **Permissions, Shadowing** indique que la règle s'applique à la fois aux contrôles d'accès et aux copie de réplication.
    - **Device Type(s)** Les types de périphériques auxquels s'applique la règle.
    - **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs client qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs client qui travaillent hors ligne.

Vous pouvez définir des règles contextuelles différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur la façon de définir les règles contextuelles hors ligne, consultez le chapitre intitulé «Gestion des règles contextuelles hors ligne pour les périphériques.»

Modification de règles contextuelles

Vous pouvez modifier les propriétés des règles contextuelles comme Description, Applies To, Device Type(s), Actions.

Pour modifier une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, cliquez droit sur **Content-Aware Rules**, cliquez sur **Manage**, puis procédez comme suit:
   a) Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
   b) Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Rules**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.
   - OU -
   Cliquez droit sur la règle, puis cliquez sur l'option **Edit** du menu de raccourcis.

   - OU -

   Dans **Devices**, développez **Content-Aware Rules**, puis procédez comme suit:
   a) Dans **Content-Aware Rules**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans le panneau de détails.

b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.

- OU -

Dans le panneau de détails, double-cliquez sur la règle à modifier.

La boîte de dialogue Edit Rule apparaît.

4. Dans la boîte de dialogue **Edit Rule**, modifiez les propriétés de règles en fonction de vos besoins.
5. Cliques sur **OK** pour valider les modifications.

Copie de règles contextuelles

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles contextuelles existantes.

Pour copier une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.

     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez copier la règle.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
5. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Rules**, sélectionnez la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Si vous utilisez la combinaison de touches CTRL+X pour couper la règle, cette règle ne sera coupée qu'une fois collée.

Pour effectuer un glisser/déposer, sélectionnez la règle et déplacez-la sur l'utilisateur ou le groupe d'utilisateurs auxquels vous désirez appliquer la règle ainsi copiée.

6. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

7. Dans la boîte de dialogue **Select Users or Groups**, champ **Enter the object names to select**, saisissez les noms des utilisateurs ou des groupes dont vous souhaitez copier la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous avez ajoutés s'affichent sous Users dans le panneau inférieur gauche de la boîte de dialogue Content-Aware Rules.

8. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous Users, sélectionnez les utilisateurs ou les groupes dont vous souhaitez copier la règle.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

9. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, cliquez droit dans le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée est affichée dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules.

10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de règles contextuelles

Vous pouvez exporter toutes vos règles contextuelles en cours dans un fichier .cwl susceptible d'être importé et utilisé sur un autre ordinateur. L'exportation et l'importation peut aussi servir à la sauvegarde.

Pour exporter des règles contextuelles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Save**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Save** de la barre d'outils.
     - OU -
   - Développez **Content-Aware Rules**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur **Save**.
     - OU -
   - Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Save**.
     - OU -
   - Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Save** de la barre d'outils.
     - OU -
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Save**.

   La boîte de dialogue Save As apparaît.

4. Dans la boîte de dialogue **Save As**, champ **Save in**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .cwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez des règles, celles-ci sont sauvegardées dans un fichier à extension .cwl.

Pour importer des règles contextuelles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Load**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Load** de la barre d'outils.
     - OU -
   - Développez **Content-Aware Rules**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur **Load**.
     - OU -
   - Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Load**.
     - OU -
   - Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Load** de la barre d'outils.
     - OU -
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Load**.

   La boîte de dialogue Open apparaît.

4. Dans la boîte de dialogue **Open**, liste **Look in**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrer le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Vous ne pouvez importer qu'un seul fichier .cwl à la fois.

Révocation de règles contextuelles

Si vous déployez les politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor, vous risquez dans certains cas de souhaiter empêcher l'application des règles contextuelles à un groupe d'ordinateurs client particulier. Pour ce faire, vous devez replacer les Content-Aware Rules précédemment définies en statut non configuré. Tous les paramètres DeviceLock révoqués sont ignorés par les ordinateurs client.

Pour révoquer des règles contextuelles

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.

b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.

c) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Undefine**.

Suppression de règles contextuelles

Vous pouvez supprimer les règles contextuelles individuelles qui ne sont plus nécessaires.

Pour supprimer une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.

   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.

   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.

   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:

   - Développez **Content-Aware Rules**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.

     Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.

     - OU -

   - Développez **Content-Aware Rules**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.

     - OU -

   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware**

Rules, sous **Rules**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.

Pour sélectionner plusieurs règles à supprimer, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

Règles contextuelles pour les protocoles (Regular Profile)

Les règles contextuelles étendent les fonctions de contrôle d'accès aux protocoles de DeviceLock en y apportant une protection supplémentaire, intuitive et au niveau du contenu des données d'entreprise contenant des informations confidentielles sur la société. Les règles contextuelles activent la vérification automatique du contenu des données et des fichiers transmis sur le réseau, la détection des contenus sensibles et l'application des politiques réglementaires afin de garantir la protection des données.

Les règles contextuelles permettent d'accorder ou de refuser, de manière sélective, l'accès à certains contenus de fichiers transmis sur le réseau, indépendamment des permissions préétablies au niveau du protocole. Les règles contextuelles permettent également d'accorder ou de refuser la copie de réplication de certains contenus. Pour plus de flexibilité, les Règles contextuelles peuvent être définies au niveau de l'utilisateur ou au niveau du groupe.

Vous pouvez configurer les règles contextuelles pour qu'elles s'appliquent aux opérations de contrôle d'accès, à celles de copie de réplication, ou aux deux.

Voici quelques exemples d'utilisation des règles contextuelles.

- **Exemple 1 – Utilisation des règles contextuelles pour opérations de contrôle d'accès**. Vous pouvez empêcher certains utilisateurs ou groupes d'utilisateurs de télécharger des fichiers contenant des numéros de carte de crédit, des numéros de téléphone ou des adresses vers des sites Web FTP.
- **Exemple 2 – Utilisation des règles contextuelles pour opérations de copie de réplication**. Vous pouvez spécifier que les conversations de messagerie instantanée comportant des numéros de cartes de crédit et des adresses email soient répliquées à des fins d'audit de sécurité et d'enquête sur les incidents.

Remarque: Vous pouvez définir des règles contextuelles différentes selon qu'il s'agit de règles Online (en ligne) ou Offline (hors ligne) pour le même utilisateur ou groupe d'utilisateurs. Les règles contextuelles en ligne (Regular Profile) s'appliquent aux ordinateurs client qui travaillent en ligne. Les règles contextuelles hors ligne (Regular Profile) s'appliquent aux ordinateurs client qui travaillent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, consultez le chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur la façon de définir les règles contextuelles pour les protocoles hors ligne, consultez le chapitre intitulé «Gestion des règles contextuelles pour les protocoles hors ligne.»

Règles contextuelles pour opérations de contrôle d'accès

Les règles contextuelles permettent d'effectuer les opérations suivantes:

- Accorder l'accès au contenu indiqué lorsque l'accès est refusé au niveau du protocole.
- Refuser l'accès au contenu indiqué lorsque l'accès est accordé au niveau du protocole.

Les règles contextuelles sont également prioritaires par rapport aux différentes règles définies dans la Liste blanche des protocoles.

Le tableau suivant présente un résumé des informations sur les droits d'accès pouvant être spécifiés pour chaque protocole dans les règles contextuelles.

PROTOCOLE	DROITS D'ACCES	DESCRIPTION
FTP	Generic: Outgoing Files	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour télécharger des fichiers avec le contenu indiqué sur un serveur FTP.
	SSL: Outgoing Files	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour télécharger des fichiers avec le contenu indiqué sur un serveur FTP en utilisant le protocole FTPS.
HTTP	Generic: POST Requests	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des données Web avec le contenu indiqué à un serveur Web en utilisant le protocole HTTP.
	Generic: Outgoing Files	Contrôle si l'utilisateur à l'autorisation nécessaire pour télécharger des fichiers avec le contenu indiqué sur un serveur Web en utilisant le protocole HTTP.
	SSL: POST Requests	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des données Web avec le contenu indiqué à un serveur Web en utilisant le protocole HTTPS.
	SSL: Outgoing Files	Contrôle si l'utilisateur à l'autorisation nécessaire pour télécharger des fichiers avec le contenu indiqué sur un serveur Web en utilisant le protocole HTTPS.
ICQ/AOL Messenger, IRC, Jabber	Generic: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des messages instantanés avec le contenu indiqué.
	SSL: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des messages instantanés avec le contenu indiqué en utilisant le protocole SSL.
Mail.ru Agent, Windows Messenger, Yahoo Messenger	Generic: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des messages instantanés avec le contenu indiqué.
SMTP, Web Mail	Generic: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des emails avec le contenu

PROTOCOLE	DROITS D'ACCES	DESCRIPTION
(messagerie Web)		indiqué.
	Generic: Outgoing Files	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des pièces jointes d'emails avec le contenu indiqué.
	SSL: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des emails avec le contenu indiqué en utilisant le protocole SSL.
	SSL: Outgoing Files	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des pièces jointes d'emails avec le contenu indiqué en utilisant le protocole SSL.
Social Networks (Réseaux sociaux)	Generic: Outgoing Messages	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des messages, des commentaires et des articles avec le contenu indiqué.
	Generic: Outgoing Files	Contrôle si l'utilisateur dispose de l'autorisation nécessaire pour envoyer des fichiers multimédia et autres avec le contenu indiqué à un site de réseau social.

Remarque: Si l'autorisation pour un protocole est du type No Access et qu'il y a une règle contextuelle permettant l'accès au contenu indiqué pour le même protocole, le droit d'accès du type Send/Receive Data est automatiquement accordé aux utilisateurs pour ce protocole. Pour plus d'informations sur ce droit d'accès, voir «Gestion d'autorisations pour protocoles.»

Tenez compte des points suivants lors de l'utilisation des règles contextuelles:

- ***Si les règles contextuelles sont définies à la fois pour les périphériques et pour les protocoles, toutes les vérifications d'accès seront exécutées en un seul traitement***.
- ***Les règles contextuelles avec paramètres Refuser sont prioritaires par rapport aux règles avec paramètres Autoriser si elles s'appliquent aux mêmes utilisateurs ou groupes d'utilisateurs***.
- ***Le processus de vérification du contenu des fichiers peut prendre du temps. Vous pouvez définir un «Content verification message» à afficher aux utilisateurs lorsque la vérification de contenu est en cours. Pour obtenir des informations détaillées sur ce message, lire la section «Message de vérification de contenu» dans «Options de service.»***
- ***Lorsqu'un utilisateur essaie d'utiliser un protocole auquel il n'a pas accès, il reçoit un Protocols blocked message, si le paramètre Protocols blocked message est activé dans Service Options. Pour obtenir des informations détaillées sur ce message, lire la section «Message en cas de blocage de protocoles» dans «Options de service.»***

Règles contextuelles pour opérations de copie de réplication

Pour pouvoir utiliser les règles contextuelles pour opérations de copie de réplication, vous devez activer l'option **Auditing and Shadowing** au niveau du protocole. Les règles contextuelles s'appliquant aux opérations de copie de réplication filtrent les copies de réplication des données et des fichiers transmis par l'utilisateur.

Le tableau suivant présente un résumé des informations sur les droits de réplication pouvant être spécifiés pour chaque protocole dans les règles contextuelles.

PROTOCOLE	DROITS DE REPLICATION	DESCRIPTION
FTP	Generic: Incoming Files	Contrôle si les fichiers avec le contenu indiqué téléchargés à partir d'un serveur FTP doivent ou non être répliqués.
	Generic: Outgoing Files	Contrôle si les fichiers avec le contenu indiqué téléchargés vers un serveur FTP doivent ou non être répliqués.
	SSL: Incoming Files	Contrôle si les fichiers avec le contenu indiqué téléchargés à partir d'un serveur FTP en utilisant le protocole FTPS doivent ou non être répliqués.
	SSL: Outgoing Files	Contrôle si les fichiers avec le contenu indiqué téléchargés vers un serveur FTP en utilisant le protocole FTPS doivent ou non être répliqués.
HTTP	Generic: Incoming Files	Contrôle si les fichiers avec le contenu indiqué téléchargés à partir d'un serveur Web doivent ou non être répliqués.
	Generic: POST Requests	Contrôle si des données Web avec le contenu indiqué soumises à un serveur Web doivent ou non être répliquées.
	Generic: Outgoing Files	Contrôle si les fichiers avec le contenu indiqué téléchargés vers un serveur Web doivent ou non être répliqués.
	SSL: Incoming Files	Contrôle si les fichiers avec le contenu indiqué téléchargés à partir d'un serveur Web en utilisant le protocole HTTPS doivent ou non être répliqués.
	SSL: POST Requests	Contrôle si des données Web avec le contenu indiqué soumises à un serveur Web en utilisant le protocole HTTPS doivent ou non être répliquées.
	SSL: Outgoing Files	Contrôle si les fichiers avec le contenu indiqué téléchargés vers un serveur Web en utilisant le protocole HTTPS doivent ou non être répliqués.
ICQ/AOL Messenger,	Generic: Incoming Messages	Contrôle si les messages instantanés avec le contenu indiqué reçus par un utilisateur doivent ou non être

PROTOCOLE	DROITS DE REPLICATION	DESCRIPTION
IRC, Jabber		répliqués.
	Generic: Outgoing Messages	Contrôle si les messages instantanés avec le contenu indiqué envoyés par un utilisateur doivent ou non être répliqués.
	SSL: Incoming Messages	Contrôle si les messages instantanés avec le contenu indiqué reçus par un utilisateur en utilisant le protocole SSL doivent ou non être répliqués.
	SSL: Outgoing Messages	Contrôle si les messages instantanés avec le contenu indiqué envoyés par un utilisateur en utilisant le protocole SSL doivent ou non être répliqués.
Mail.ru Agent, Windows Messenger, Yahoo Messenger	Generic: Incoming Messages	Contrôle si les messages instantanés avec le contenu indiqué reçus par un utilisateur doivent ou non être répliqués.
	Generic: Outgoing Messages	Contrôle si les messages instantanés avec le contenu indiqué envoyés par un utilisateur doivent ou non être répliqués.
SMTP, Web Mail (messagerie Web)	Generic: Outgoing Messages	Contrôle si les emails avec le contenu indiqué envoyés par un utilisateur doivent ou non être répliqués.
	Generic: Outgoing Files	Contrôle si les pièces jointes d'emails avec le contenu indiqué envoyées par un utilisateur doivent ou non être répliquées.
	SSL: Outgoing Messages	Contrôle si les emails avec le contenu indiqué envoyés par un utilisateur en utilisant le protocole SSL doivent ou non être répliqués.
	SSL: Outgoing Files	Contrôle si les pièces jointes d'emails avec le contenu indiqué envoyées par un utilisateur en utilisant le protocole SSL doivent ou non être répliquées.
Social Networks (Réseaux sociaux)	Generic: Outgoing Messages	Contrôle si les messages, les commentaires et les articles avec le contenu indiqué envoyés par un utilisateur doivent ou non être répliqués.
	Generic: Outgoing Files	Contrôle si les fichiers avec le contenu indiqué téléchargés vers un site de réseau social doivent ou non être répliqués.

Configuration de paramètres de détection de contenu

Les règles contextuelles sont créées sur la base de groupes de contenus permettant de définir, de façon centralisée, les types de contenus pour lesquels vous désirez appliquer des restrictions d'accès. Les groupes de contenus indiquent le critère de filtrage à utiliser pour la sélection des données auxquelles les règles doivent s'appliquer.

Tous les groupes de contenus sont stockés dans la base de contenus. La même base de contenus est utilisée à la fois pour les périphériques et pour les protocoles. La base de contenus fait partie de la politique DeviceLockService et est également enregistrée dans un fichier XML, avec les paramètres de service que l'on peut créer à partir de DeviceLock Management Console, de DeviceLock Service Settings Editor ou de DeviceLock Group Policy Manager.

Il existe plusieurs types de groupes de contenus: Les groupes File Type Detection, les groupes Keywords, les groupes Pattern, les groupes Document Properties et les groupes Complex. Ces différents groupes, ainsi que leur mode d'utilisation, sont décrits dans les sections ci-dessous.

Groupes File Type Detection Content

Les groupes File Type Detection servent à contrôler l'accès aux fichiers au niveau typologique. Ces groupes contiennent les définitions des types de fichiers qui les constituent. Une définition de type de fichier comporte deux propriétés: une extension de nom de fichier (par exemple, DOC) et une description (par exemple, document Microsoft Word). Lorsque vous définissez une règle basée sur un groupe File Type Detection, elle s'applique à tous les types de fichiers contenus dans ce groupe.

DeviceLock comprend 34 groupes File Type Detection prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
Archives	MS Outlook & Outlook Express
Audio, Video & Flash	MS PowerPoint
BlackBerry	MS Project
Common Object File Format (COFF)	MS Publisher
Database	MS Visio
Executable	MS Windows Installer
Fax Documents	MS Windows Memory Dump
FileMaker Pro	MS Word
Fonts	MS Works
Help Files	OpenOffice, StarOffice, OpenDocument, etc.
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
Lotus SmartSuite	QuickBooks, Quicken, TurboTax & etc.
MS Access	Rich Text Format
MS Excel	Security Certificates
MS InfoPath	Text, HTML & XML
MS Money	Virtual Machines
MS OneNote	WordPerfect Office

Remarque: Les règles contextuelles prennent en charge les formats Word To Go, Sheet To Go et Slideshow To Go des périphériques Palm. Le format Word To Go est inclus dans les groupes de contenus intégrés MS Word et Rich Text Format, le format Sheet To Go est inclus dans le groupe de contenus intégré MS Excel, alors que le format Slideshow To Go est inclus dans le groupe de contenus intégré MS PowerPoint.

Les fichiers Microsoft Word ou Rich Text Format (RTF), les fichiers Excel et les fichiers PowerPoint peuvent être transférés à un périphérique Palm à l'aide de l'application Documents To Go. L'application Documents To Go convertit ces fichiers dans des formats spéciaux: Les fichiers Word et RTF sont convertis au format Word To Go, les fichiers Excel sont convertis au format Sheet To Go, et les fichiers PowerPoint sont convertis au format Slideshow To Go. Les fichiers convertis sont automatiquement téléchargés sur le Palm lorsque les utilisateurs se synchronisent.

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les définitions de type de fichier contenues dans les groupes File Type Detection intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création de groupes de détection de types de fichiers personnalisés

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes de contenus de détection de types de fichiers personnalisés permettent de spécifier les types de fichiers que vous souhaitez inclure dans le même groupe afin de mieux répondre aux besoins particuliers de votre entreprise.

Supposez par exemple que vous deviez autoriser certains utilisateurs à accéder aux documents Word, Excel et PDF, ainsi qu'aux fichiers graphiques. Pour ce faire, commencez par créer un nouveau groupe de contenus comportant ces types de contenus. Puis, définissez une règle en fonction du groupe de contenus ainsi personnalisé.

Pour créer un groupe de détection de types de fichiers personnalisés

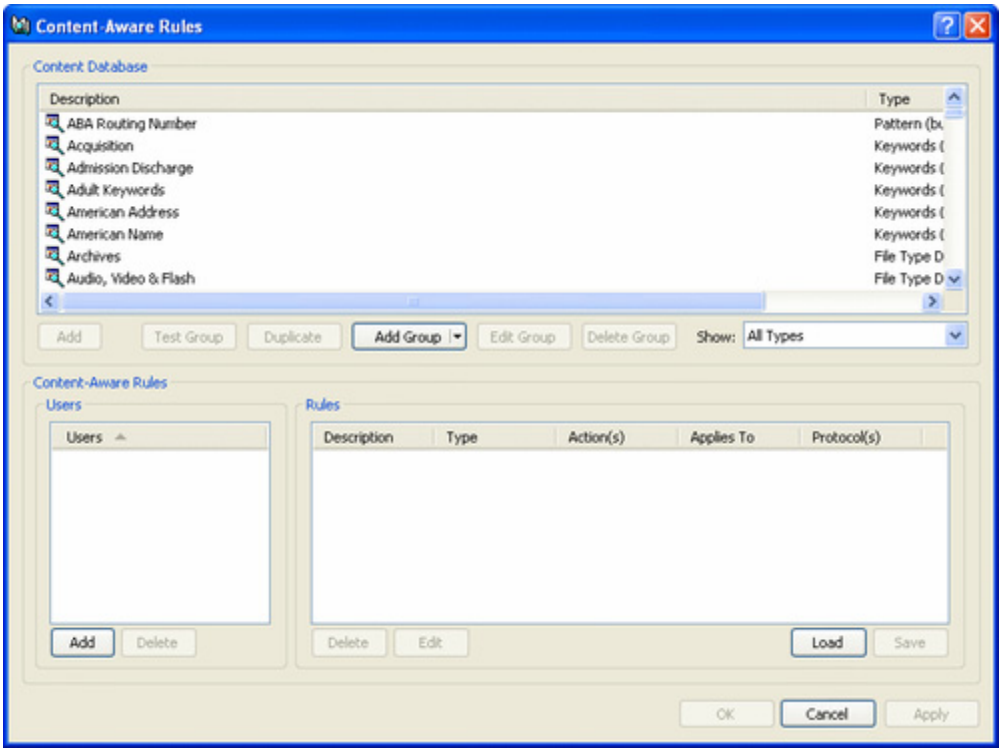
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.

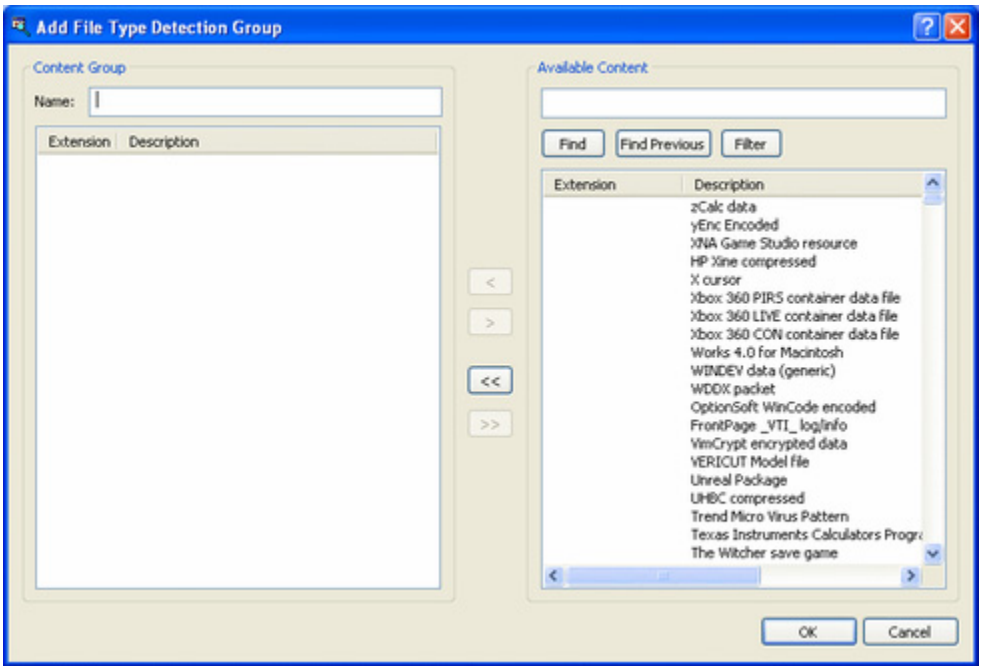
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **File Type Detection**.

   La boîte de dialogue Add File Type Detection Group apparaît.



5. Dans le panneau de gauche de la boîte de dialogue **Add File Type Detection Group**, sous **Content group**, saisissez le nom du nouveau groupe de contenus dans la boîte **Name**.
6. Dans le panneau de droite de la boîte de dialogue **Add File Type Detection Group**, sous **Available Content**, sélectionnez tous les types de fichiers que vous souhaitez ajouter au nouveau groupe de contenus, puis cliquez sur le bouton comportant une flèche simple orientée vers la gauche [<].

   Pour sélectionner plusieurs types de fichiers, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

   Pour supprimer des types de fichiers individuels du groupe de contenus, utilisez le bouton comportant une flèche simple orientée vers la droite [>]. Pour ajouter ou supprimer d'un seul coup tous les types de fichiers disponibles dans le groupe de contenus, utilisez le bouton comportant une flèche double orientée vers la gauche [<<] ou vers la droite [>>].

   Remarque: Vous pouvez rechercher les types de fichiers disponibles dans la base de contenus par extension ou par description. Vous pouvez utiliser des caractères génériques comme les astérisques (*) et les points d'interrogation (?) pour rechercher un groupe ou des types de fichiers donnés. Pour trouver un type ou un groupe de types de fichiers donné, dans **Available Content**, saisissez une extension ou une description avec ou sans caractères génériques dans la séquence de recherche, puis cliquez sur **Find**. Pour filtrer les types de fichiers, cliquez sur **Filter**. Pour supprimer le filtre, appliquez-le à une séquence vide.

   L'astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser ces caractères génériques n'importe où et en nombre illimité.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Add File Type Detection Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la

boîte de dialogue Content-Aware Rules.

Groupes de contenus Keywords

Les groupes Keywords sont utilisés pour contrôler l'accès aux données et aux fichiers en fonction des mots clés ou des expressions indiqués.

DeviceLock comprend 157 groupes Keywords prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss
Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property
American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation
Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital
Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses
Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver's License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments

GROUPES DE CONTENUS INTEGRES	
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medicinal Active Substances
FITS Date & Time	Russian: Medicinal Drugs
FITS File Checksum	Russian: Noncompliant
FITS File Descriptors	Russian: Passwords and Access Codes
FITS Hierarchical file grouping	Russian: Physical Security
FITS Instrumentorum	Russian: Prices
FITS Non-standard	Russian: Project Documentation
FITS Observations	Russian: Project Names
FITS Standard	Russian: Project Versions
Gambling	Russian: Projects Release Date
Grades	Russian: Technology
HCFA (CMS) 1500 Form	Russian: User Names
HIPAA - Diseases	Russian: Working Conditions
HIPAA HCPCS	Sales Forecast
HIPAA ICD9	Sarbanes-Oxley Sensitive
HIPAA NDC Classes	Security
HIPAA NDC Dosages	Security Agencies
HIPAA NDC Listing	Sensitive Disease
HIPAA NDC Routes	Sexual Language
Illegal Drugs	Social Security
Innovations	SPAM
Internet Slang Abbreviations	Sports
Investments	Staff Training
Java Source Code	Substance Abuse
Market Development	Suspicious Activity Report
Medical Diagnosis	Technology
Medical Record Numbers	UBO4 Form
MEMO	US Birth Date
Network Security	US Birth Place
Partner Names	US Expiry Date
Password	User Name
Payments	VB Source Code
PCI GLBA	Violence
Perl Source Code	Weapon Keywords
Price List	Wire Transfer
Prices	Working Conditions
Pro Earnings	

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les mots clés contenus dans les groupes Keywords intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création d'un groupe Keywords personnalisé

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes de contenus Keywords personnalisés

permettent de spécifier les mots clés que vous souhaitez inclure dans le même groupe afin de mieux répondre aux besoins particuliers de votre entreprise.

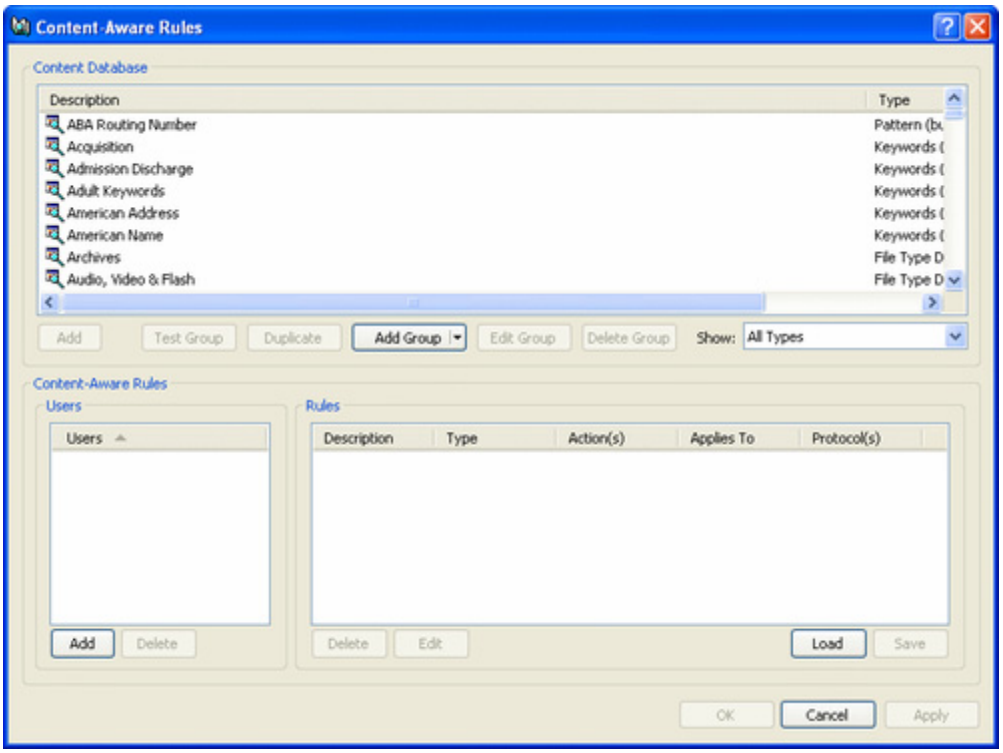
Pour créer un groupe Keyword personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

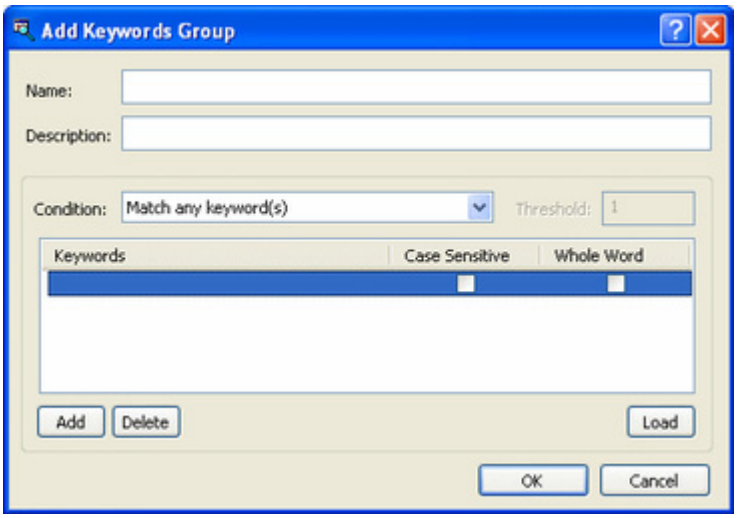
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Keywords**.

   La boîte de dialogue Add Keywords Group apparaît.



5. Dans la boîte de dialogue **Add Keywords Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
Condition:	Préciser les conditions d'application des règles associées à ce groupe de contenu. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Condition:** • **Match any keyword(s)** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que l'un des mots clés spécifiés figure dans les données de texte. • **Match all keyword(s)** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que tous les mots clés spécifiés figurent dans les données de texte. • **Only when combined score exceeds (or equal to) threshold** – indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre total (la somme) des occurrences de tous les mots clés figurant dans les données de texte égale ou dépasse le nombre maximum d'occurrences des mots clés.
Threshold	Indiquer un nombre maximum d'occurrences des mots clés. Ce nombre peut varier entre 0 et 65535. Ce paramètre doit être renseigné si vous avez sélectionné l'option **Only when combined score exceeds (or equal to) threshold**.
Keywords	Indiquer les mots ou les expressions à rechercher dans le texte des données. Double-cliquez sur **Keywords** pour saisir un mot clé ou une expression.

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Case Sensitive	Préciser la sensibilité à la casse des mots clés. Cochez la case **Case Sensitive** pour activer la sensibilité à la casse (à titre d'exemple, les mots «test» et «Test» seront considérés comme étant des mots clés différents). Décochez la case **Case Sensitive** pour désactiver la sensibilité à la casse (à titre d'exemple, les mots «test» et «Test» seront considérés comme étant un même mot clé).
Whole Word	Indiquer les options de correspondance du mot clé. Cochez la case **Whole Word** pour activer l'option de correspondance exacte (permet de rechercher une correspondance exacte du mot clé). Décochez la case **Whole Word** pour désactiver l'option de correspondance exacte (permet de rechercher des variantes grammaticales du mot clé).
Weight	Indiquer le degré d'importance de chaque mot clé ou expression. Le paramètre Weight sert à compter le nombre d'occurrences des mots clés spécifiés dans le texte des données. Ce paramètre doit être renseigné si vous avez sélectionné l'option **Only when combined score exceeds (or equal to) threshold**. Valeurs possibles: **Heavy**, **Above Normal**, **Normal** (valeur par défaut), **Below Normal**, **Light**. Ces valeurs du paramètre Weight peuvent être interprétées de la manière suivante: **Heavy**: indique que chaque occurrence est comptabilisée trois fois. C'est la valeur la plus élevée. **Above Normal**: indique que chaque occurrence est comptabilisée deux fois. **Normal**: indique que chaque occurrence est comptabilisée une fois. **Below Normal**: indique que deux occurrences comptent pour une. **Light**: indique que trois occurrences comptent pour une. C'est la valeur la plus faible.
Add	Indiquer les mots clés et les expressions clés. Cliquez sur **Add** pour entrer un mot clé ou une expression clé.
Delete	Supprimer un mot clé. Pour ce faire, sélectionnez le mot clé que vous souhaitez supprimer et cliquez sur **Delete**. Pour sélectionner plusieurs mots clés, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
Load	Importer une liste de mots clés à partir d'un fichier TXT.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Keywords Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes de contenus Pattern

Les groupes de contenus Pattern permettent de contrôler l'accès à des fichiers de données en utilisant des modèles de texte décrits par des expressions régulières Perl. Ces modèles fournissent un moyen, flexible et efficace, de détection automatique des contenus sensibles (par exemple, les numéros de cartes de crédit, les numéros de sécurité sociale, les adresses email et les numéros de téléphone) dans les textes des données.

Pour plus d'informations sur la création et l'utilisation des expressions régulières Perl, veuillez consulter le Tutoriel rapide sur les expressions régulières Perl et le Tutoriel sur les expressions régulières Perl (en anglais).

DeviceLock comprend 45 groupes Pattern prédéfinis (intégrés) permettant de configurer les autorisations et/ou les autorisations de copie de réplication à votre convenance. Vous pouvez utiliser les groupes de contenus intégrés tels qu'ils sont, en créer des copies (duplications) modifiables, ou encore créer vos propres groupes de contenus selon les besoins particuliers de votre entreprise.

Ces groupes prédéfinis sont énumérés dans le tableau suivant:

GROUPES DE CONTENUS INTEGRES	
ABA Routing Number	Russian: Main State Registration Number
BIC (ISO 9362)	Russian: Motorcycle Numbers
Canadian Social Insurance Number	Russian: Passport
Credit Card Number	Russian: Pension Insurance Number
Email Address	Russian: Post Code
European VAT Number	Russian: Taxpayer Identification Number
GPS Data (RMC String)	Russian: Telephone Number
IBAN	Russian: Trailer Numbers
International Telephone Number	Russian: Vehicle Registration Document
IP Address	SQL Queries
ISO Date	TCP/UDP Port Number
MAC Address	Time (12/24h)
Microsoft Windows Product Key	UK National Insurance Number
Russian: Address	UK Phone Number
Russian: Auto Insurance Number	UK Post Code
Russian: Bank Account Number	UK Tax Code
Russian: BIC	Uniform Resource Locator (URL)
Russian: Car Numbers	US Date
Russian: Classification of Economic Activities	US Phone Number
Russian: Classification of Enterprises and Organizations	US Social Security Number
Russian: Driver's License Number	US Zip Code
Russian: Health Insurance Number	VIN
Russian: International Passport	

Les groupes de contenus intégrés permettent de créer et d'appliquer des règles sans avoir à définir vos propres groupes de contenus.

Remarque: Vous pouvez voir les modèles d'expressions régulières contenus dans les groupes Pattern intégrés, mais vous ne pouvez ni les modifier ni les supprimer. Pour plus d'informations sur la façon de consulter les groupes de contenus intégrés, voir «Consulter les groupes de contenus intégrés.»

Création d'un groupe Pattern personnalisé

Vous pouvez définir des règles contextuelles en fonction de vos propres groupes de contenus (personnalisés) si les groupes de contenus prédéfinis figurant dans DeviceLock ne correspondent pas à vos besoins. Les groupes Pattern personnalisés permettent de préciser le modèle que vous souhaitez utiliser pour identifier des informations sensibles dans un texte de données.

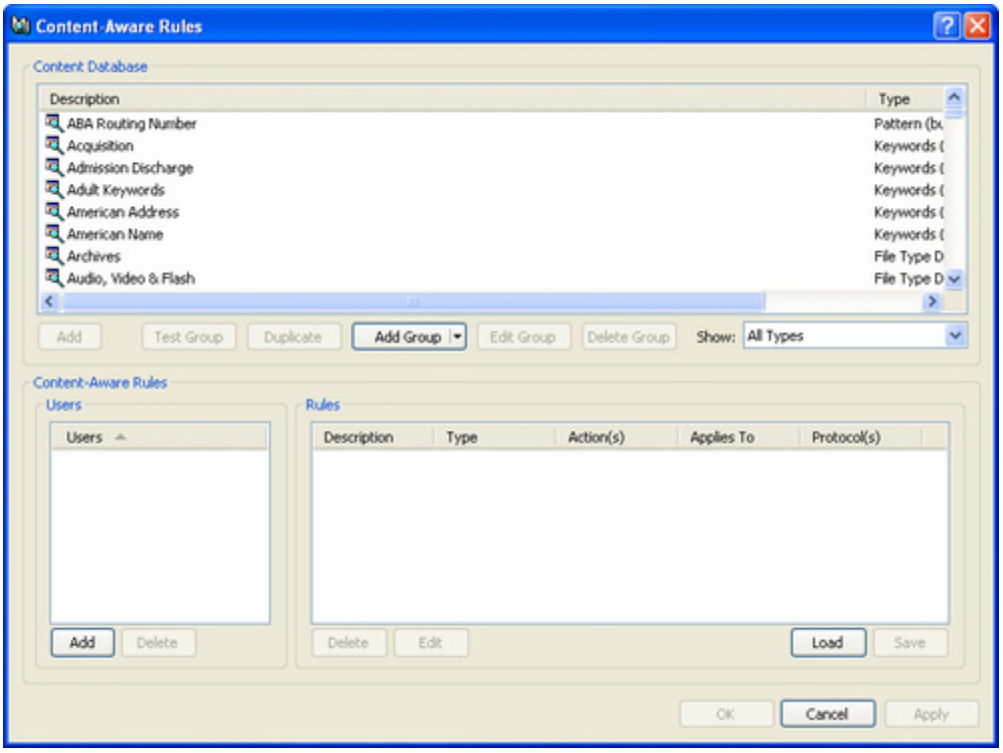
Pour créer un groupe Pattern personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

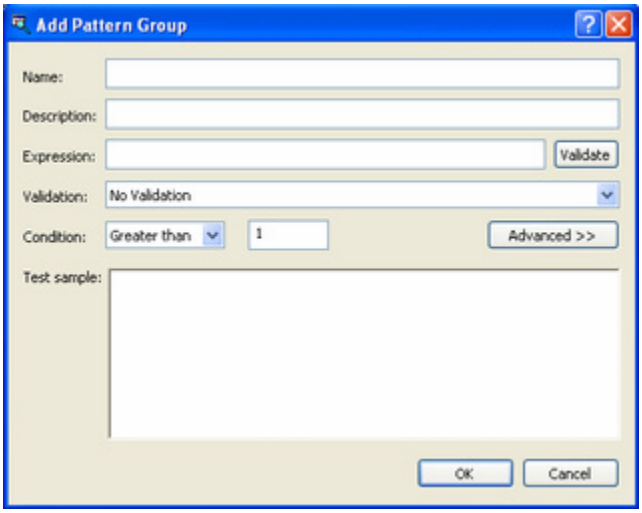
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Pattern**.

   La boîte de dialogue Add Pattern Group apparaît.



5. Dans la boîte de dialogue **Add Pattern Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Description:	Donner une description pour le groupe.
Expression	Indiquer le modèle en créant une expression régulière. Pour plus d'informations sur la création des expressions régulières Perl, veuillez consulter le Tutoriel rapide sur les expressions régulières Perl et le Tutoriel sur les expressions régulières Perl (en anglais).
Validate	Vérifier la syntaxe de l'expression régulière.
Validation	Effectuer la validation réelle des correspondances potentielles renvoyées par l'expression régulière. Les options suivantes sont disponibles: **No validation** (Cette option est sélectionnée par défaut.), **ABA Routing Number**, **Canadian Social Insurance Number**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Date, Date (ISO)**, **Email Address**, **European VAT Number**, **IBAN**, **IP Address**, **LUHN Checksum**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations**, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social Security Number**.
Condition:	Préciser les conditions d'application des règles associées à ce groupe de contenu. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Condition**: • **Less than or =** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est inférieur ou égal au nombre spécifié. • **Equal to** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est égal au nombre spécifié. • **Greater than or =** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière est supérieur ou égal au nombre spécifié. • **Between** indique qu'une règle associée à ce groupe de contenus est activée chaque fois que le nombre de correspondances renvoyées par l'expression régulière se trouve dans la plage spécifiée.
Advanced	Effectuer un test rapide du modèle de l'expression régulière sur des données-échantillon. Cliquez sur **Advanced** pour afficher ou masquer la boîte **Test sample**.
Test sample	Entrer une chaîne à tester et voir le résultat. DeviceLock prend en charge la mise en surbrillance de couleur en temps réel des résultats. Tous les résultats concordants sont surlignés en vert, tandis que les

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
	chaînes qui ne correspondent pas au modèle sont surlignées en rouge.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Pattern Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes de contenus Document Properties

Les groupes Document Properties permettent de contrôler l'accès aux fichiers en fonction des propriétés des fichiers telles que le nom, la taille du fichier... Ils permettent également de contrôler l'accès aux documents et aux archives protégés par mot de passe, ainsi qu'aux images textes.

Remarque: Le ET logique s'applique à toutes les propriétés des fichiers contenus dans un groupe Document Properties. À titre d'exemple, si vous voulez contrôler l'accès aux fichiers de plus de 5 mégaoctets (Mo) et aux documents et archives protégés par mot de passe, vous devez créer deux groupes Document Properties distincts : un groupe pour le contrôle d'accès aux fichiers de plus de 5 Mo et un groupe pour le contrôle d'accès aux documents et aux archives protégés par mot de passe. Si vous spécifiez ces propriétés de fichiers dans le même groupe Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera les documents et les archives protégés par mot de passe dont la taille est supérieure à 5 Mo.

DeviceLock n'intègre pas de groupe de contenus Document Properties prédéfinis. La procédure suivante indique comment créer un groupe Document Properties.

Pour créer un groupe Document Properties

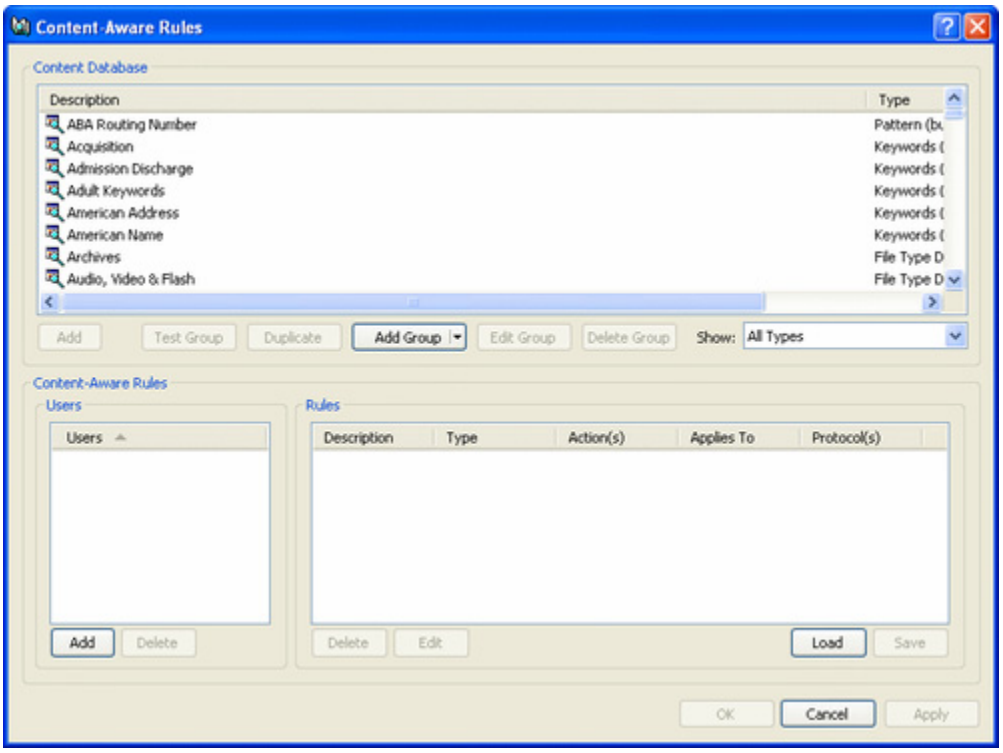
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -

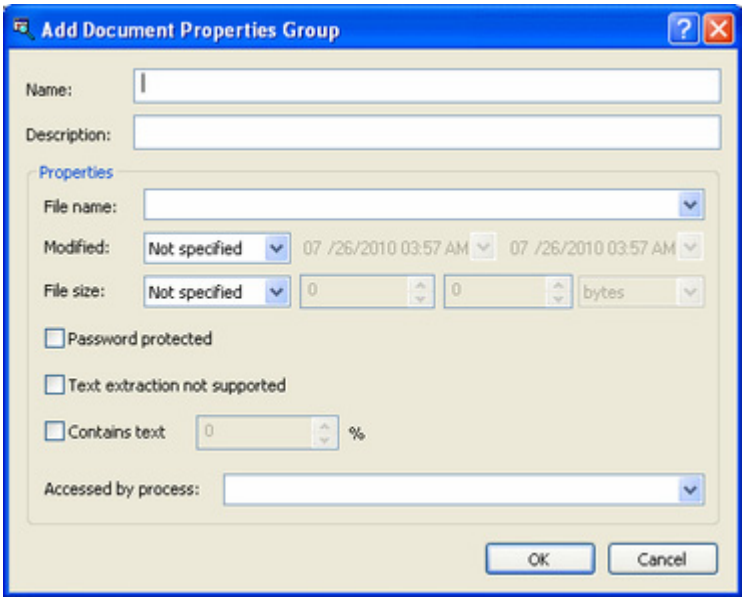
- Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Document Properties**.

La boîte de dialogue Add Document Properties Group apparaît.



5. Dans la boîte de dialogue **Add Document Properties Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
File name	Indiquer le nom des fichiers. Vous pouvez utiliser des jokers comme les astérisques (*) et les points d'interrogation (?). Par exemple, saisissez ***.txt** pour indiquer tous les fichiers avec l'extension .txt Les différents noms de fichiers doivent être séparés par un point-virgule (;), par exemple: ***.doc; *.docx**. *L'astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple*.
Modified	Indiquer la dernière date et heure de modification du fichier. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **Modified**: • **Not specified** (cette option est sélectionnée par défaut). • **Before than**: indique que la date et l'heure de modification du fichier doivent être antérieures à la date et à l'heure indiquées. • **After than**: indique que la date et l'heure de modification du fichier doivent être ultérieures à la date et à l'heure indiquées. • **Between**: indique que la date et l'heure de modification du fichier doivent être comprises dans la plage indiquée. • **Not older than**: indique que la date et l'heure de modification du fichier ne doivent pas être plus grands que le nombre de secondes, minutes, jours, semaines, mois et années indiqué. • **Older than**: indique que la date et l'heure de modification du fichier doivent être plus grands que le nombre de secondes, minutes, jours, semaines, mois et années indiqué. **Remarque:** La propriété **Modified** ne s'applique pas aux fichiers transmis via le réseau. Même invoquée, elle est ignorée lors de l'analyse de contenus.
File size	Indiquer la taille du fichier en octets, kilo-octets, méga-octets, giga-octets ou téra-octets. Pour ce faire, cliquez sur l'une des options suivantes dans la liste **File size**: • **Not specified** (cette option est sélectionnée par défaut). • **Equal to**: indique que les fichiers doivent être d'une taille égale à la taille indiquée. • **Less than**: indique que les fichiers doivent être d'une taille inférieure à la taille indiquée. • **More than**: indique que les fichiers doivent être d'une taille supérieure à la taille indiquée. • **Between**: indique que la taille des fichiers doit se situer dans la plage indiquée.
Password protected	Détecter et contrôler l'accès aux archives, fichiers PDF et documents Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx) protégés par mot de passe. Si vous cochez la case **Password protected** pour un groupe

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
	Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera l'accès aux archives, fichiers PDF et documents Microsoft Office protégés par mot de passe. Décochez la case **Password protected** si vous ne souhaitez pas détecter et contrôler l'accès aux archives, fichiers PDF et documents Microsoft Office protégés par mot de passe. Pour plus d'informations sur les formats d'archives pris en charge, veuillez lire la description de la fonction «Vérification des fichiers contenus dans les archives.»
Text extraction not supported	Contrôler l'accès aux formats de fichiers non pris en charge. Si vous cochez la case **Text extraction not supported** pour un groupe Document Properties, puis créez une règle contextuelle basée sur ce groupe de contenus, cette règle contrôlera l'accès à tous les fichiers à format non pris en charge. Tous les formats pris en charge sont énumérés dans la section «Extension des fonctionnalités de DeviceLock avec ContentLock et NetworkLock.»
Contains text	Détecter et contrôler l'accès aux images selon qu'elles contiennent ou non du texte. Si vous cochez la case **Contains text** pour un groupe Document Properties, puis créez une règle contextuelle basée sur la combinaison de ce groupe de contenus et du groupe de contenus d'images intégrées et de dessins et autres fichiers CAD par l'opérateur logique AND, cette règle vérifiera si les images prises en charge contiennent du texte et contrôlera l'accès aux images contenant du texte. Décochez la case **Contains text** si vous ne souhaitez pas détecter et contrôler l'accès aux images contenant du texte. Pour plus d'informations sur les formats d'images pris en charge, veuillez lire la description de la fonction «Détection de texte dans les images.» Vous devez préciser la quantité de texte que les images doivent contenir si vous cochez la case **Contains text**. La quantité de texte est exprimée en pourcentage de la superficie totale de l'image. Par exemple, si le texte occupe la moitié de l'image, la quantité de texte sera 50 %. Si une image n'est constituée que de texte (document scanné par exemple), la quantité de texte est de 100 %. **Remarque:** L'option **Contains text %** s'applique également aux autres formats de fichiers pris en charge. Dans ce cas, le pourcentage est le rapport entre la taille du texte en caractères et la taille du fichier en octets.
Accessed by process	Indiquer le nom du processus en train d'accéder au fichier du document. Vous pouvez utiliser des jokers comme les astérisques (*) et les points d'interrogation (?). Les différents noms de processus doivent être séparés par un point-virgule (;), par exemple: **explorer.exe; notepad.exe**.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Document Properties Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Groupes à contenus complexes

Les groupes à contenus complexes utilisent des expressions booléennes pour sélectionner les documents pour lesquels vous désirez contrôler l'accès. Ces groupes peuvent inclure toute combinaison de groupes de contenus intégrés ou personnalisés (groupes File Type Detection, Keywords, Pattern et Document Properties) connectés par un nombre quelconque d'opérateurs logiques. Chaque groupe de contenus est considéré comme un critère de filtre unique que vous pouvez inclure dans l'expression booléenne. L'utilisation de groupes de contenus multiples permet de créer des filtres complexes pour identifier les contenus sensibles dans les données transmises sur le réseau.

Le tableau suivant répertorie les opérateurs logiques dans l'ordre de priorité décroissant.

OPERATEUR	SIGNIFICATION
NOT	Négation logique d'un critère de filtre
AND	Application simultanée des deux filtres
OR	Application de l'un ou l'autre critère de filtre

Vous pouvez utiliser des parenthèses pour modifier la priorité des opérateurs et forcer l'évaluation de certaines parties de l'expression avant les autres. Les critères imbriqués dans des parenthèses sont évalués de l'intérieur vers l'extérieur. DeviceLock prend en charge l'imbrication à plusieurs niveaux des critères. Un groupe complexe peut contenir au maximum 30 groupes de contenus.

DeviceLock n'intègre pas de groupe de contenus complexes prédéfinis. La procédure suivante indique comment créer un groupe complexe.

Pour créer un groupe complexe

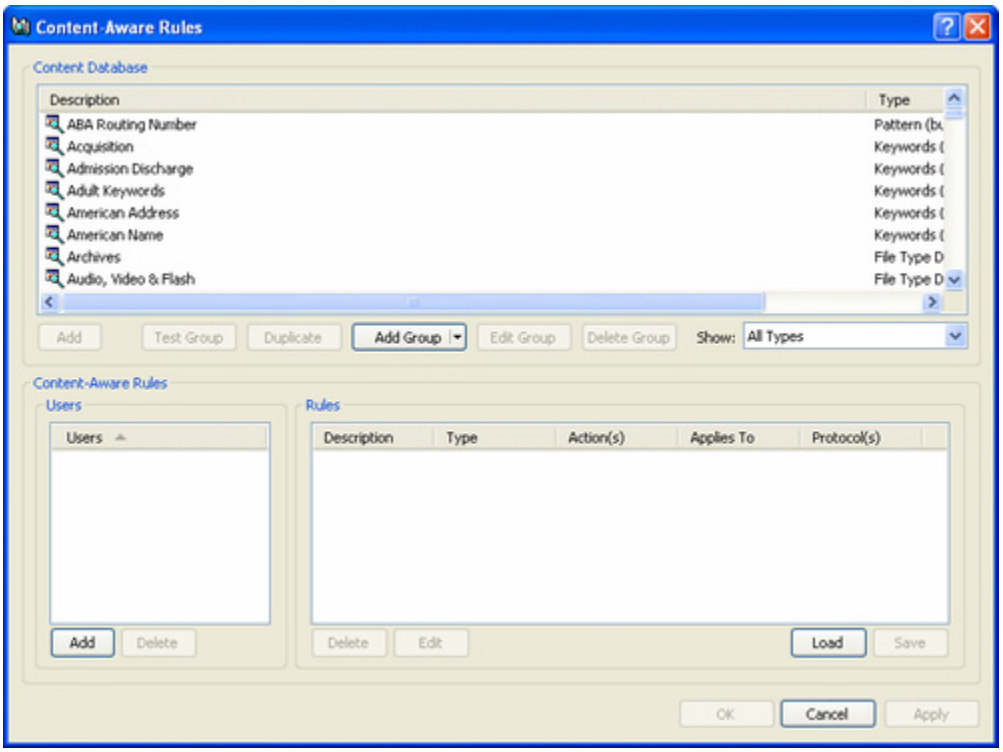
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
    a) Ouvrez Group Policy Object Editor.
    b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
    - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
    - OU -

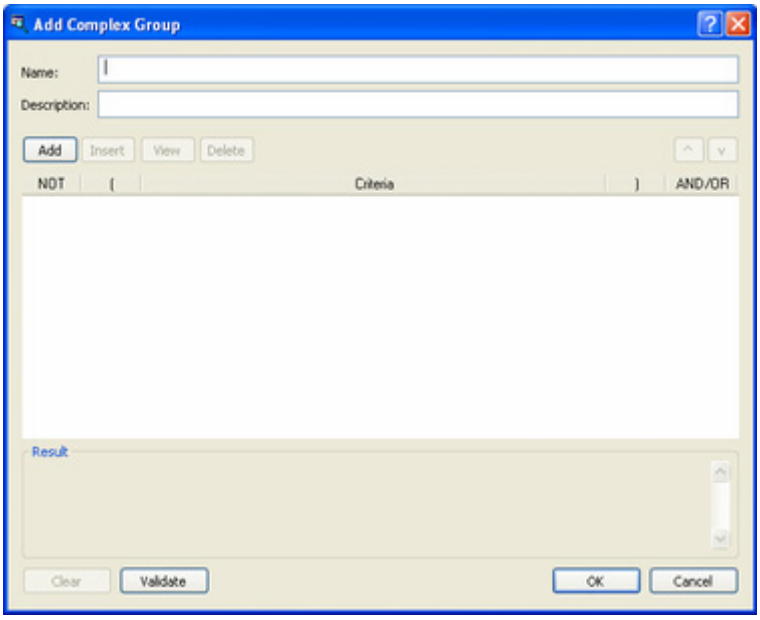
- Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, cliquez sur la flèche déroulante à côté de l'option **Add Group**, puis sur **Complex**.

   La boîte de dialogue Add Complex Group apparaît.



5. Dans la boîte de dialogue **Add Complex Group**, procédez comme suit:

UTILISEZ CE PARAMETRE	POUR FAIRE CECI
Name	Indiquer le nom du groupe.
Description:	Donner une description pour le groupe.
Add	Ajouter des groupes de contenus à partir de la base de contenus. Pour ce faire, cliquez sur **Add** pour ouvrir la boîte de dialogue **Content Groups**. Dans le champ **Content Database** de la boîte de dialogue **Content Groups**, sélectionnez le groupe désiré et cliquez sur **OK**. *Pour sélectionner plusieurs groupes de contenus, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. *Pour voir les informations concernant un groupe de contenus, sélectionnez le groupe concerné et cliquez sur View Group*. *Les groupes de contenus que vous avez ajoutés apparaissent dans la colonne Criteria de la boîte de dialogue Add Complex Group. Chaque groupe de contenus que vous ajoutez est considéré comme un critère de filtre unique que vous pouvez inclure dans l'expression booléenne*.
Insert	Insérer un groupe de contenus, avant le groupe actuellement sélectionné dans la colonne **Criteria**, à partir de la base de contenus. Pour ce faire, cliquez sur Insert pour ouvrir la boîte de dialogue **Content Groups**. Dans le champ **Content Database** de la boîte de dialogue **Content Groups**, sélectionnez le groupe désiré et cliquez sur **OK**.
View	Voir les informations concernant le groupe actuellement sélectionné dans la colonne **Criteria**.
Delete	Supprimer le groupe sélectionné de la colonne **Criteria**.
NOT	Appliquer l'opérateur logique NOT à chaque groupe sélectionné. Pour ce faire, sélectionnez le groupe de votre choix dans la colonne **Criteria** et cochez la case appropriée dans la colonne **Not**.
AND/OR	Appliquer l'opérateur logique AND ou l'opérateur logique OR à chaque groupe sélectionné. Pour ce faire, sélectionnez le groupe de votre choix dans colonne **Criteria** et cochez la case appropriée dans la colonne **AND/OR**.
Clear	Effacer la liste de groupes de contenus actuelle dans la colonne **Criteria**.
Validate	Valider votre expression. Si l'expression n'a pas été définie proprement (il existe par exemple une parenthèse ouvrant ne correspondant à aucune parenthèse fermante), un message d'erreur s'affichera.

6. Cliquez sur **OK** pour fermer la boîte de dialogue **Add Complex Group**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Consulter les groupes de contenus intégrés

Vous pouvez consulter tous les groupes de contenus intégrés, mais vous ne pouvez ni les modifier ni les supprimer.

Pour voir un groupe de contenus intégré

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
    a) Ouvrez Group Policy Object Editor.
    b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
    - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
      - OU -
    - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

    La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez un groupe de contenus intégré que vous souhaitez consulter, puis cliquez sur **View Group**.

Dupliquer les groupes de contenus intégrés

Vous ne pouvez pas modifier les groupes de contenus intégrés. Toutefois, vous pouvez en créer des copies éditables (duplications), pour répondre aux besoins particuliers de votre entreprise.

Pour dupliquer un groupe de contenus intégré

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
    a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
    a) Ouvrez DeviceLock Service Settings Editor.
    b) Dans l'arborescence, développez **DeviceLock Service**.

    Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus que vous souhaitez dupliquer, puis cliquez sur **Duplicate**.
5. Dans la boîte de dialogue qui s'ouvre alors, effectuez les changements nécessaires, puis cliquez sur **OK**.

   Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database du panneau supérieur de la boîte de dialogue Content-Aware Rules.

Modification et suppression d'un groupe de contenus personnalisé

Vous pouvez à tout moment modifier ou supprimer des groupes de contenus personnalisés.

Pour modifier ou supprimer un groupe de contenus personnalisé

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.

4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus personnalisé que vous souhaitez modifier ou supprimer.
5. Cliquez sur **Edit Group** pour modifier le groupe de contenu sélectionné. Dans la boîte de dialogue qui s'ouvre alors, effectuez les changements nécessaires puis cliquez sur **OK**.

   - OU -

   Cliquez sur **Delete Group** ou appuyez sur la touche DELETE (Suppr) pour supprimer le groupe de contenus sélectionné.
6. Dans la boîte de dialogue **Content-Aware Rules**, cliquez sur **OK** ou sur **Apply** pour appliquer les modifications.

Test des groupes de contenus

Vous pouvez tester n'importe quel groupe de contenus intégré ou personnalisé pour vérifier si les fichiers spécifiés y correspondent effectivement. Ces tests permettent de vérifier si les règles contextuelles créées sur la base de ces groupes répondent aux exigences particulières de votre entreprise.

Pour tester un groupe de contenus

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.
4. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus que vous souhaitez tester, puis cliquez sur **Test Group**.

   Vous ne pouvez tester qu'un seul groupe de contenus à la fois.

   La boîte de dialogue Open apparaît.

5. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez utiliser pour tester le groupe de contenus spécifié.
6. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
7. Cliquez sur le fichier, puis sur **Open**.

   La boîte de message des résultats s'affiche. Si le fichier concorde avec le groupe de contenus indiqué, la boîte de message des résultats affichera le texte suivant: «Selected file matches with the group.» Si le fichier ne concorde pas avec le groupe de contenus indiqué, la boîte de message des résultats affichera le texte suivant: «Selected file does not match with the group.»

   Lorsque le test est en cours, la console ne répond plus (elle se bloque).

Gestion des règles contextuelles

La gestion des règles contextuelles comprend les tâches suivantes:

- Définition de règles contextuelles
- Modification de règles contextuelles
- Copie de règles contextuelles
- Exportation et importation de règles contextuelles
- Révocation de règles contextuelles
- Suppression de règles contextuelles

Les règles contextuelles peuvent être créées à l'aide de DeviceLock Management Console, de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor.

Définition de règles contextuelles

Les règles contextuelles sont créées sur la base des groupes de contenus intégrés ou sur la base des groupes de contenus personnalisés. Pour plus d'informations sur ces groupes, voir «Configuration des paramètres de détection de contenu.»

Pour définir une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

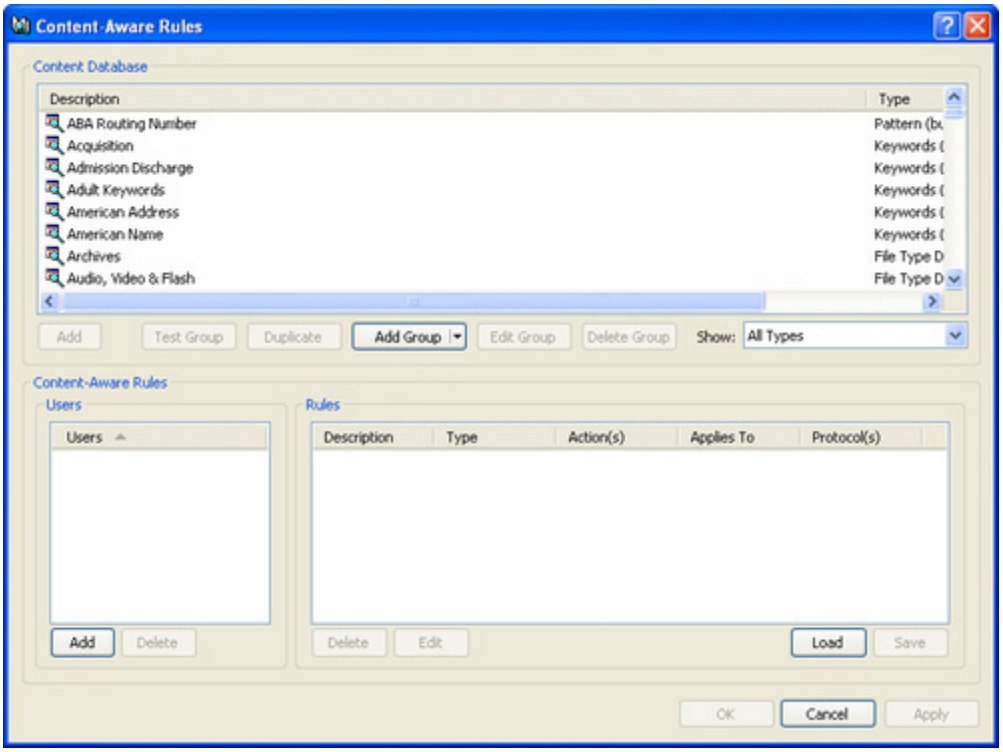
   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.



4. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau inférieur gauche de la boîte de dialogue Content-Aware Rules.

   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, puis cliquez sur **Delete** ou appuyez sur la touche DELETE (Suppr).

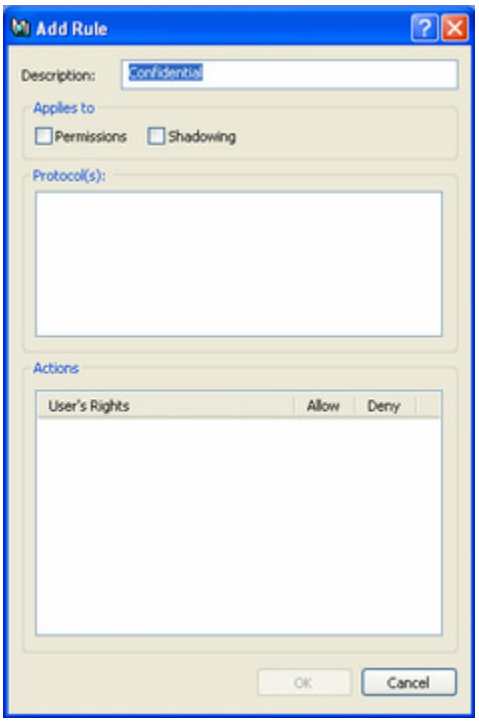
6. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sélectionnez les utilisateurs ou les groupes pour lesquels vous souhaitez définir la règle.

Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules**, sélectionnez le groupe de contenus souhaité, puis cliquez sur **Add**.

   Remarque: Vous ne pouvez indiquer qu'un seul groupe de contenus par règle contextuelle.

   La boîte de dialogue Add Rule apparaît.



8. Dans le champ **Description** de la boîte de dialogue **Add Rule**, saisissez le nom de la règle contextuelle.

   Par défaut, la règle contextuelle a le même nom que le groupe de contenus indiqué mais vous pouvez saisir un nom différent.

9. Dans **Applies to**, indiquez le type d'opération associé à la règle. Les options disponibles sont les suivantes:

   - **Permissions**: Indique que la règle s'appliquera aux opérations de contrôle d'accès.
   - **Shadowing**: Indique que la règle s'appliquera aux opérations de copie de réplication.
   - **Permissions, Shadowing**: Indique que la règle s'appliquera aux opérations de contrôle d'accès et de copie de réplication.

10. Dans **Protocol(s)**, sélectionnez le ou les types de protocoles auxquels vous souhaitez que cette règle s'applique.

    Les règles contextuelles peuvent s'appliquer aux protocoles suivants: FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, Réseaux sociaux, messagerie Web, Windows Messenger, et Yahoo Messenger.

Si plusieurs protocoles sont sélectionnés dans le paramètre Action(s), la boîte de dialogue affichera uniquement les droits d'accès qui sont communs à tous les protocoles sélectionnés.

11. Dans le champ **Action(s)**, indiquez les actions utilisateur qui sont autorisées ou non sur les protocoles, et celles qui sont consignées dans le journal de réplication.

    Pour en savoir plus sur les droits d'utilisateur susceptibles de figurer dans les règles contextuelles, consultez les chapitres intitulés «Règles contextuelles pour opérations de contrôle d'accès» et «Règles contextuelles pour opérations de copie de réplication.»

12. Cliquez sur **OK**.

    La règle ainsi créée s'affiche dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules.

13. Cliquez sur **OK** ou **Apply** pour appliquer la règle.

    Les utilisateurs ou les groupes auxquels s'applique la règle contextuelle figurent dans la section Content-Aware Rules de l'arborescence. Si vous sélectionnez un utilisateur ou un groupe auquel la règle contextuelle s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

    - **Description** Le nom de la règle. Par défaut, la règle a le même nom que le groupe de contenus indiqué.
    - **Type** Le type de l'analyse de contenus. Valeurs possibles: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, et **Complex**. **File Type Detection** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs signatures propres. **Keywords** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des mots clés et des expressions spécifiés. **Pattern** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des modèles de textes décrits par les expressions régulières Perl. **Document Properties** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs propriétés. **Complex** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction du contenu décrit par une expression booléenne.
    - **Action(s)** affiche les actions utilisateur qui sont autorisées ou non sur les protocoles, et celles qui sont consignées dans le journal de réplication.
    - **Applies To** Valeurs possibles: **Permissions**, **Shadowing**, et **Permissions, Shadowing**. **Permissions** indique que la règle s'applique aux contrôles d'accès. **Shadowing** indique que la règle s'applique aux copies de réplication. **Permissions, Shadowing** indique que la règle s'applique à la fois aux contrôles d'accès et aux copie de réplication.
    - **Protocol(s)** Les protocoles auxquels s'applique la règle.
    - **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs client qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs client qui travaillent hors ligne.

      Vous pouvez définir des règles contextuelles différentes selon qu'elles s'appliquent en ligne ou hors ligne au même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur la façon de définir les règles contextuelles pour les protocoles hors ligne, consultez le chapitre intitulé «Gestion des règles contextuelles pour les protocoles hors ligne.»

Modification de règles contextuelles

Vous pouvez modifier les propriétés des règles contextuelles, notamment les propriétés Description, Applies To, Protocol(s), Actions.

Pour modifier une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **Content-Aware Rules**, cliquez sur **Manage**, puis procédez comme suit:
   a) Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
   b) Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Rules**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.
   - OU -
   Cliquez droit sur la règle, puis cliquez sur l'option **Edit** du menu de raccourcis.

   - OU -

   Dans **Protocols**, développez **Content-Aware Rules**, puis procédez comme suit:
   a) Dans **Content-Aware Rules**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans le panneau de détails.
   b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.
   - OU -
   Dans le panneau de détails, double-cliquez sur la règle à modifier.

   La boîte de dialogue Edit Rule apparaît.

4. Dans la boîte de dialogue **Edit Rule**, modifiez les propriétés de règles en fonction de vos besoins.
5. Cliques sur **OK** pour valider les modifications.

Copie de règles contextuelles

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles contextuelles existantes.

Pour copier une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules apparaît.

4. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez copier la règle.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.

5. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Rules**, sélectionnez la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

   La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

   Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Si vous utilisez la combinaison de touches CTRL+X pour couper la règle, cette règle ne sera coupée qu'une fois collée.

Pour effectuer un glisser/déposer, sélectionnez la règle et déplacez-la sur l'utilisateur ou le groupe d'utilisateurs auxquels vous désirez appliquer la règle ainsi copiée.

6. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

7. Dans la boîte de dialogue **Select Users or Groups**, champ **Enter the object names to select**, saisissez les noms des utilisateurs ou des groupes dont vous souhaitez copier la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous avez ajoutés s'affichent sous Users dans le panneau inférieur gauche de la boîte de dialogue Content-Aware Rules.

8. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous Users, sélectionnez les utilisateurs ou les groupes dont vous souhaitez copier la règle.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

9. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, cliquez droit dans le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée est affichée dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules.

10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de règles contextuelles

Vous pouvez exporter toutes vos règles contextuelles en cours dans un fichier .cwl susceptible d'être importé et utilisé sur un autre ordinateur. L'exportation et l'importation peut aussi servir à la sauvegarde.

Pour exporter des règles contextuelles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Save**.
  - OU -
- Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Save** de la barre d'outils.
  - OU -
- Développez **Content-Aware Rules**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur **Save**.
  - OU -
- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Save**.
  - OU -
- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Save** de la barre d'outils.
  - OU -
- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Save**.

La boîte de dialogue Save As apparaît.

4. Dans la boîte de dialogue **Save As**, champ **Save in**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .cwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez des règles, celles-ci sont sauvegardées dans un fichier à extension .cwl.

Pour importer des règles contextuelles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Load**.

- OU -

- Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Load** de la barre d'outils.

  - OU -

- Développez **Content-Aware Rules**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur **Load**.

  - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Load**.

  - OU -

- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Load** de la barre d'outils.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Users**, cliquez sur **Load**.

La boîte de dialogue Open apparaît.

4. Dans la boîte de dialogue **Open**, liste **Look in**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrer le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Vous ne pouvez importer qu'un seul fichier .cwl à la fois.

Révocation de règles contextuelles

Si vous déployez les politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou de DeviceLock Service Settings Editor, vous risquez dans certains cas de souhaiter empêcher l'application des règles contextuelles à un groupe d'ordinateurs client particulier. Pour ce faire, vous devez replacer les Content-Aware Rules précédemment définies en statut non configuré. Tous les paramètres DeviceLock révoqués sont ignorés par les ordinateurs client.

Pour révoquer des règles contextuelles

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Undefine**.

Suppression de règles contextuelles

Vous pouvez supprimer les règles contextuelles individuelles qui ne sont plus nécessaires.

Pour supprimer une règle contextuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Développez **Content-Aware Rules**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.
     Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.

     - OU -
   - Développez **Content-Aware Rules**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.
     - OU -
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules**, sous **Users**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules**, sous **Rules**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.
     Pour sélectionner plusieurs règles à supprimer, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

Protocoles (Regular Profile)

DeviceLock permet de contrôler les données transférées via d'autres protocoles de réseau, d'où une meilleure protection contre la publication non désirée d'informations et une sécurité accrue des conditions de transport. La fonctionnalité Protocoles, permet de définir les politiques servant à autoriser ou à bloquer, de manière sélective, la transmission de données ou de fichiers par l'intermédiaire de certains protocoles, ainsi que la réplication des donnés transférées. Pour une meilleure flexibilité, il est possible de définir les politiques par utilisateur ou par groupe.

DeviceLock permet de contrôler les protocoles et applications Web suivantes:

- **FTP** (Protocole de transfert de fichiers) Le protocole Internet standard de transfert de fichiers entre ordinateurs.

  Les connexions FTP en mode actif et en mode passif sont prises en charge. FTPS (FTP sur SSL) est aussi pris en charge. Les connexions FTPS implicites et explicites sont prises en charge.
- **HTTP** (Protocole de transfert hypertexte) Un protocole d'application client/serveur utilisé pour transférer des informations sur Internet.

  HTTPS (SSL sur HTTP) est aussi pris en charge.
- **ICQ/ AOL Messenger** Le système ouvert d'AOL pour la communication en temps réel (OSCAR) utilisé par ICQ et AOL Instant Messenger (AIM).

  Les connexions non-SSL et SSL sont prises en charge.
- **IRC** (Internet Relay Chat) Un protocole Internet standard qui prend en charge les communications de texte interactives en temps réel dans les «salles de chat» établies sur Internet au moyen de serveurs IRC.

  Les connexions non-SSL et SSL sont prises en charge.
- **Jabber** Un protocole XML ouvert de messagerie instantanée.

  Les connexions non-SSL et SSL sont prises en charge.
- **Mail.ru Agent** Un programme de messagerie instantanée créé par Mail.ru.
- **SMTP** (Simple Mail Transfer Proto) Un protocole Internet standard utilisé pour échanger des messages électroniques entre serveurs SMTP sur Internet.

  Le mode SMTP étendu (ESMTP) est aussi pris en charge. Les connexions non-SSL et SSL sont prises en charge.
- **Social Networks** Contrôle les communications avec les sites de réseaux sociaux. Les sites de réseaux sociaux suivants sont pris en charge: Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING.

  Remarque: Le trafic SSL sur les sites de réseaux sociaux est contrôlé comme un trafic générique (non-SSL).
- **Telnet** Le protocole Internet standard d'émulation de terminal à distance.

- **Web Mail** Contrôle la messagerie électronique. Les messageries électroniques suivantes sont prises en charge: Gmail, AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, et Yandex Mail.
  Les connexions non-SSL et SSL sont prises en charge.
- **Windows Messenger** Microsoft Notification Protocol (MSNP) utilisé par Windows Live Messenger et Windows Messenger.
- **Yahoo Messenger** Le protocole de réseau utilisé par la messagerie instantanée Yahoo! Messenger de Yahoo!

Remarque: Le protocole SSL est utilisé dans la liste blanche de protocoles afin de permettre la connexion des applications à certificats SSL intégrés à leur serveur respectif.

Vous pouvez gérer les politiques de sécurité des protocoles à l'aide des utilitaires DeviceLock Management Console, Service Settings Editor ou DeviceLock Group Policy Manager. Vous pouvez aussi utiliser le plug-in Report Permissions/Auditing de DeviceLock Enterprise Server pour visualiser et changer les politiques de sécurité définies pour les protocoles. Pour en savoir plus, reportez-vous au chapitre «Report Permissions/Auditing.»

Gestion des autorisations de protocoles

Pour administrer l'échange d'informations de la couche transport, configurez l'accès aux protocoles de communication en définissant les autorisations appropriées. Ces autorisations indiquent les restrictions d'accès et le niveau d'accès appliqués aux utilisateurs. Les autorisations peuvent être définies par utilisateur ou par groupe.

La table suivante indique les droits d'accès disponibles pour les autorisations associées aux protocoles.

PROTOCOLE	DROITS D'ACCÈS
FTP	**Generic: Send/Receive Data** Le droit de se connecter à un serveur FTP, d'envoyer et de recevoir des données de protocole, de télécharger des fichiers à partir d'un serveur FTP. **Generic: Outgoing Files** Le droit de télécharger des fichiers sur un serveur FTP. **SSL: Send/Receive Data** Le droit de se connecter à un serveur FTP, d'envoyer et de recevoir des données du protocole, de télécharger des fichiers à partir d'un serveur FTP à l'aide du protocole FTPS. **SSL: Outgoing Files** Le droit de télécharger des fichiers sur un serveur FTP à l'aide du protocole FTPS.
HTTP	**Generic: Send/Receive Data** Le droit de se connecter à un serveur Web, d'envoyer et de recevoir des données du protocole, des pages Web et des objets sur les pages Web (scripts, fichiers Flash, JPEG, PNG, et images GIF, etc.). **Generic: POST Requests** Le droit d'envoyer des données Web à un serveur Web à l'aide du protocole HTTP. **Generic: Outgoing Files** Le droit de télécharger des fichiers sur un serveur Web à l'aide du protocole HTTP.

PROTOCOLE	DROITS D'ACCÈS
	SSL: Send/Receive Data Le droit de se connecter à un serveur Web, d'envoyer et de recevoir des données du protocole, des pages Web et des objets sur les pages Web (scripts, fichiers Flash, JPEG, PNG, et images GIF, etc.) à l'aide du protocole HTTPS. **SSL: POST Requests** Le droit d'envoyer des données Web à un serveur Web à l'aide du protocole HTTPS. **SSL: Outgoing Files** Le droit de télécharger des fichiers sur un serveur Web à l'aide du protocole HTTPS.
ICQ/AOL Messenger	**Generic: Send/Receive Data** Le droit de se connecter au serveur ICQ et AOL Instant Messenger et de recevoir des messages instantanés. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé. **SSL: Send/Receive Data** Le droit de se connecter au serveur ICQ et AOL Instant Messenger et de recevoir des messages instantanés à l'aide du protocole SSL. **SSL: Outgoing Messages** Le droit d'envoyer des messages instantanés à l'aide du protocole SSL. Le transfert de fichiers n'est pas contrôlé.
IRC	**Generic: Send/Receive Data** Le droit de se connecter au serveur IRC et de recevoir des messages instantanés. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé. **SSL: Send/Receive Data** Le droit de se connecter au serveur IRC à l'aide du protocole SSL. **SSL: Outgoing Messages** Le droit d'envoyer des messages instantanés à l'aide du protocole SSL. Le transfert de fichiers n'est pas contrôlé.
Jabber	**Generic: Send/Receive Data** Le droit de se connecter au serveur Jabber et de recevoir des messages instantanés. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé. **SSL: Send/Receive Data** Le droit de se connecter au serveur Jabber à l'aide du protocole SSL. **SSL: Outgoing Messages** Le droit d'envoyer des messages instantanés à l'aide du protocole SSL. Le transfert de fichiers n'est pas contrôlé.
Mail.ru Agent	**Generic: Send/Receive Data** Le droit de se connecter au serveur Mail.ru Agent to the Mail.ru et de recevoir des messages instantanés. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé.
SMTP	**Generic: Send/Receive Data** Le droit de se connecter au serveur SMTP, d'envoyer et de recevoir des données du protocole. **Generic: Outgoing Messages** Le droit d'envoyer des emails sans pièces jointes. **Generic: Outgoing Files** Le droit d'envoyer des pièces jointes d'emails. **SSL: Send/Receive Data** Le droit de se connecter au serveur SMTP, d'envoyer et de recevoir des données du protocole à l'aide du protocole SSL.

PROTOCOLE	DROITS D'ACCÈS
	SSL: Outgoing Messages Le droit d'envoyer des emails sans pièces jointes à l'aide du protocole SSL. **SSL: Outgoing Files** Le droit d'envoyer des pièces jointes d'emails à l'aide du protocole SSL.
Social Networks (Réseaux Sociaux)	**Generic: Send/Receive Data** Le droit d'avoir un accès visuel à un site de réseau social. **Generic: Outgoing Messages** Le droit d'envoyer des messages, des commentaires, des articles, etc. **Generic: Outgoing Files** Le droit de télécharger des fichiers multimédia et autres sur un site de réseau social.
Telnet	**Generic: Send/Receive Data** Le droit de se connecter au serveur Telnet, d'envoyer et de recevoir des données du protocole.
Web Mail	**Generic: Send/Receive Data** Le droit d'accéder à la messagerie Web et de lire des emails. **Generic: Outgoing Messages** Le droit d'envoyer des emails sans pièces jointes. **Generic: Outgoing Files** Le droit d'envoyer des pièces jointes d'emails. **SSL: Send/Receive Data** Le droit d'accéder à la messagerie Web et de lire des emails à l'aide du protocole SSL. **SSL: Outgoing Messages** Le droit d'envoyer des emails sans pièces jointes à l'aide du protocole SSL. **SSL: Outgoing Files** Le droit d'envoyer des pièces jointes d'emails à l'aide du protocole SSL.
Windows Messenger	**Generic: Send/Receive Data** Le droit de se connecter au serveur Windows Messenger. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé.
Yahoo Messenger	**Generic: Send/Receive Data** Le droit de se connecter au serveur Yahoo Messenger. **Generic: Outgoing Messages** Le droit d'envoyer des messages instantanés. Le transfert de fichiers n'est pas contrôlé.

Remarque: Vous pouvez définir des autorisations différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les autorisations en ligne (Regular Profile) s'appliquent aux ordinateurs client qui fonctionnent en ligne. Les autorisations hors ligne (Offline Profile) s'appliquent aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des autorisations hors ligne, reportez-vous au chapitre intitulé «Gestions des autorisations hors ligne de protocoles.»

Vous pouvez configurer les autorisations par défaut pour les deux types de profils (Regular Profile et Offline Profile). Les autorisations par défaut sont assignées aux comptes

Administrators et Everyone. La table suivante contient les droits d'accès accordés à ces comptes par défaut.

COMPTE/ PROTOCOLE	ADMINISTRATEURS	TOUS
FTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data SSL: Send/Receive Data
HTTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data SSL: Send/Receive Data
ICQ/AOL Messenger	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
IRC	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Jabber	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Mail.ru Agent	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages
SMTP	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Social Networks	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Telnet	Generic: Send/Receive Data	Generic: Send/Receive Data
Web Mail	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Windows Messenger	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages
Yahoo Messenger	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages

La gestion des autorisations en ligne (regular) comprend les tâches suivantes:

- Définition et édition d'autorisations
- Révocation d’autorisations

Les autorisations en ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les autorisations ne sont pas définies
Configured	Indique que les autorisations sont définies
Full Access	Indique que le compte Everyone (tout le monde) bénéficie de tous les droits d'accès.
No Access	Indique une des situations suivantes: • Le compte Everyone (tout le monde) bénéficie d'autorisations No Access (pas d'accès) et est le seul compte assigné à un protocole. *Les autorisations No Access (pas d'accès) assignées au compte Everyone (tout le monde) l'emportent sur les autorisations assignées aux autres comptes.* • Tous les utilisateurs et les groupes assignés à un protocole bénéficient d'autorisations No Access (pas d'accès). • Tous les utilisateurs et les groupes assignés à un protocole sont supprimés.

Définition et édition d'autorisations

Définir et éditer des autorisations

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l’ordinateur qui exécute DeviceLock Service.
   b) Dans l’arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l’arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l’arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations en ligne (regular) de chaque protocole dans la colonne Regular.

4. Dans le panneau de détails, procédez comme suit:
   - Cliquez droit sur le protocole pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur **Set Permissions**.
     - - OU -
   - Sélectionnez le protocole pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur le bouton **Set Permissions** de la barre d'outils.

   Pour sélectionner plusieurs protocoles afin de définir les mêmes autorisations, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

   Remarque: Quand vous sélectionnez des protocoles qui ont des droits d'accès différents, tenez compte des points suivants:

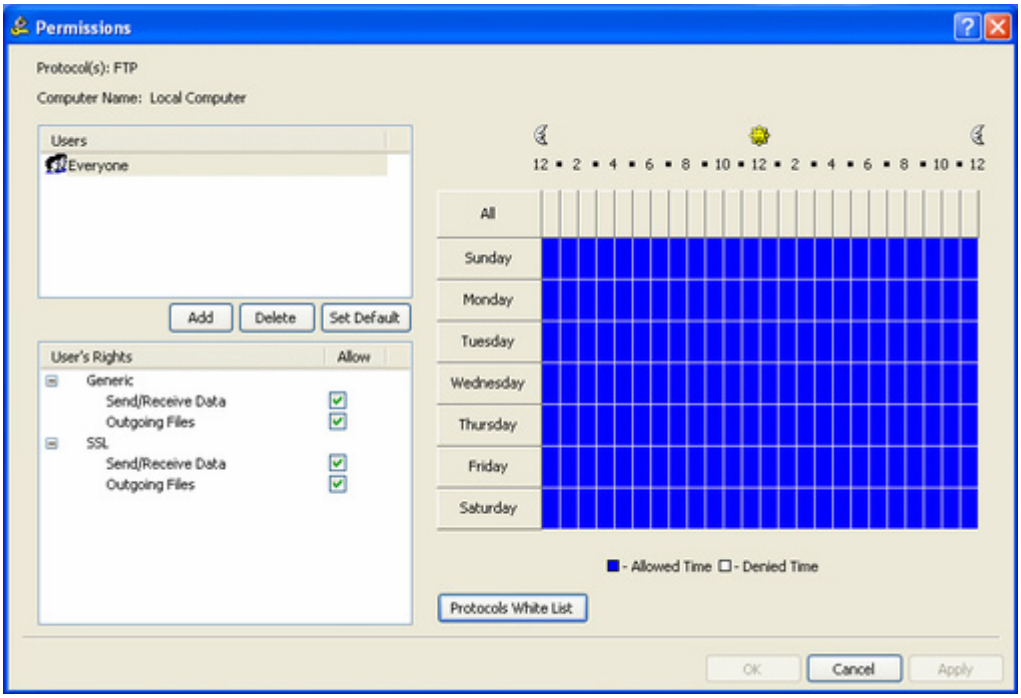
   La boîte de dialogue **Permissions** affiche uniquement les droits d'accès qui sont communs à tous les protocoles sélectionnés.

   Si tous les droits d'accès affichés dans la boîte de dialogue **Permissions** sont autorisés pour des utilisateurs particuliers, ceux–ci auront un accès libre aux protocoles sélectionnés.

   Si tous les droits d'accès affichés dans la boîte de dialogue **Permissions** sont refusés pour des utilisateurs particuliers, ceux–ci n'auront pas accès aux protocoles sélectionnés.

   Certains droits d'accès dépendent d'autres droits. Si vous accordez un droit qui nécessite un autre droit, le droit requis est accordé automatiquement. Par exemple, si vous accordez le droit **Generic: Outgoing Files** aux protocoles des réseaux sociaux et de la messagerie Web, les droits suivants sont accordés automatiquement: **Generic: Send/Receive Data**, **Generic: Outgoing Messages**, **Generic: Outgoing Files**.

   La boîte de dialogue Permissions apparaît.



5. Dans la boîte de dialogue **Permissions**, procédez comme suit:

ACTION	PROCEDURE
Définir des autorisations par défaut	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Set Default**. *Les autorisations par défaut sont assignées aux comptes Administrators et Everyone. Pour en savoir plus sur les autorisations définies pour ces comptes par défaut, consultez le chapitre intitulé* «Gestion des autorisations de protocoles.»
Définir des autorisations pour un utilisateur ou un groupe supplémentaire	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît*. 2. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes ajoutés figurent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Permissions*. 3. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue **Permissions**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs et/ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. 4. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Permissions**, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés. *Le panneau de droite de la boîte de dialogue Permissions permet de définir les limites d'accès des utilisateurs aux protocoles en termes de jours et d'heures. Utilisez le bouton gauche de la souris pour sélectionner les jours et les horaires pendant lesquels l'utilisateur ou le groupe sélectionné aura accès aux protocoles. Utilisez le bouton droit de la souris pour indiquer les jours et les horaires pendant lesquels l'utilisateur ou le groupe sélectionné n'aura pas accès aux protocoles*.
Changer les autorisations d'un utilisateur ou d'un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés.
Supprimer un utilisateur ou un groupe existant et ses autorisations	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation d'autorisations

Si vous déployez des politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou DeviceLock Service Settings Editor, dans certaines situations vous pouvez empêcher

l'application de toute ou partie des autorisations précédemment définies à certains groupes d'ordinateurs client. Pour ce faire, vous devez redonner aux autorisations précédemment définies le statut non configuré. Tous les paramètres DeviceLock non définis sont ignorés par les ordinateurs clients.

Pour révoquer des autorisations

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des autorisations.
4. Dans le panneau de détails, cliquez droit sur le protocole dont vous voulez révoquer les autorisations, puis cliquez sur **Undefine**.

   Vous pouvez révoquer les autorisations de plusieurs protocoles en même temps. Pour ce faire, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine**.

Gestion des règles d'audit et de réplication de protocoles

DeviceLock permet l'audit et la copie de réplication des données et des fichiers transférés selon différents protocoles. L'audit et la copie de réplication sont utilisés pour surveiller et enregistrer les opérations de transfert de données critiques de sécurité. L'analyse régulière des données de journalisation permet de détecter et d'assurer un suivi des utilisations incorrectes d'informations sensibles et des interceptions de données causées par la perte ou le vol de données.

Pour l'audit et la copie de réplication de la couche de transport, DeviceLock utilise deux types de journalisation : Les journaux d'audit et les journaux de réplication. Le journal d'audit est utilisé pour contrôler l'accès aux protocoles et surveiller ce que font les utilisateurs individuels. Les données d'audit sont consignées dans le journal des évènements Windows ou dans le journal propriétaire DeviceLock, ou dans les deux à la fois. Pour indiquer le journal à utiliser, définissez le paramètre Audit log type dans le champ Service

Options. Pour visualiser les données du journal d'audit, vous pouvez utiliser DeviceLock Service Audit Log Viewer ou DeviceLock Enterprise Server Audit Log Viewer.

Le journal de réplication est utilisé pour stocker la copie complète des données et des fichiers transférés au moyen des protocoles spécifiés. Pour visualiser les données du journal de réplication, vous pouvez utiliser DeviceLock Service Shadow Log Viewer ou DeviceLock Enterprise Server Shadow Log Viewer.

L'audit et la copie de réplication des données transférées au moyen des protocoles spécifiés sont activés dans les règles d'audit et de réplication. Chaque règle associée à un protocole détermine les utilisateurs ou groupes à qui elle s'applique, ainsi que les droits d'audit et de réplication qui déterminent les actions utilisateur à auditer/répliquer.

Le journal des évènements d'audit comprend de nombreuses informations comme le type de l'évènement, la date et l'heure de l'évènement, le protocole associé, l'utilisateur associé à cet évènement, les renseignements sur le processus et les informations propres à l'évènement.

La table suivante fournit un résumé des informations concernant les droits d'audit et de réplication également spécifiés dans les règles si besoin est, et indique les informations propres à l'évènement écrites dans le journal.

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
FTP	**Audit: Connection** - active le journal d'audit des tentatives de connexion à un site FTP. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal.* **Audit: Incoming Files -** active le journal d'audit des tentatives de téléchargement d'un fichier à partir d'un site FTP. *L'action Incoming File, le chemin absolu, le nom complet du fichier (par exemple, ftp://myftp/myfile.doc), l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal.* **Audit: Outgoing Files -** active le journal d'audit des tentatives de téléchargement d'un fichier sur un site FTP. *L'action Outgoing File, le chemin absolu, le nom complet du fichier (par exemple, ftp://myftp/myfile.doc), l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal*. **Shadowing: Incoming Files -** active la copie de réplication des fichiers téléchargés à partir d'un site FTP. *Les copies de réplication des fichiers téléchargés sont consignées dans le journal.* **Shadowing: Outgoing Files -** active la copie de réplication des fichiers téléchargés sur un site FTP. *Les copies de réplication des fichiers téléchargés sont consignées dans le journal*.
HTTP	**Audit: Connection** - active le journal d'audit des tentatives d'ouverture d'une

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	page Web. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Remarque:** Quand ce droit est activé, plusieurs évènements Connection sont enregistrés dans le journal d'audit lors de la tentative d'ouverture de page Web. Ceci parce qu'une page Web a souvent besoin de ressources (comme des images, des scripts, etc.) d'autres hôtes. **Audit : Incoming Data** - permet l'enregistrement de l'audit de pages Web et d'objets sur des pages Web : scripts, fichiers Flash (jusqu'à 1.5 Mo en taille), images (jusqu'à 512 Ko en taille), texte (jusqu'à 200 Ko en taille), etc. *L'action Incoming Data, l'URL de la page Web, les objets sur la page Web, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal.* **Audit: Incoming Files** - active le journal d'audit des tentatives de téléchargement d'un fichier à partir d'un site Web. *L'action Incoming File, le chemin absolu, le nom complet du fichier (par exemple, http://domain/path/myfile.doc), l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal.* **Audit: Outgoing Data** - le contenu des données sortantes ne comporte aucune donnée. Ce droit permet l'enregistrement de l'audit des tentatives bloquées d'utilisateur pour ouvrir une page Web, si l'option **Audit Denied** est réglée pour ce protocole. *L'action Outgoing Data, l'URL de la page Web, les objets sur la page Web, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal.* **Audit: POST Requests -** active le journal d'audit des tentatives d'envoi des données Web sur un site Web. *L'action POST Request et l'URL du script qui a envoyé le POST request sont consignés dans le journal.* **Audit: Outgoing Files** - active le journal d'audit des tentatives de téléchargement d'un fichier sur un site Web. *L'action Outgoing File, le chemin absolu, le nom complet du fichier (par exemple, http://domain/path/myfile.doc), l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal.* **Shadowing: Incoming Data** - permet la copie de réplication de pages Web et d'objets sur des pages Web : scripts, fichiers Flash (jusqu'à 1.5 Mo en taille), images (jusqu'à 512 Ko en taille), texte (jusqu'à 200 Ko en taille), etc. *Les copies de réplication de pages Web et leurs composants sont écrits dans le journal*. **Shadowing: Incoming Files** - active la copie de réplication des fichiers téléchargés à partir d'un site Web. *Les copies de réplication des fichiers téléchargés sont consignées dans le journal*. **Shadowing: Outgoing Data** - Ce droit n'a aucune conséquence sur la copie de

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	réplication. *Les copies de réplication des demandes HTTP sont consignées dans le journal*. **Shadowing: POST Requests -** active la copie de réplication des données Web saisies. *Les copies de réplication des données Web saisies sont consignées dans le journal*. **Shadowing: Outgoing Files** - active la copie de réplication des fichiers téléchargés sur un site Web. *Les copies de réplication des fichiers téléchargés sont consignées dans le journal*.
ICQ/AOL Messenger	**Audit: Connection** - active le journal d'audit des tentatives de connexion au serveur ICQ et AOL Instant Messenger. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception des messages instantanés. *Le Chat, l'ID de tous les participants MI, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'ID du participant local précède l'ID du participant à distance*. **Shadowing: Incoming Messages** - active la copie de réplication des messages instantanés reçus. *Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus.* **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.
IRC	**Audit: Connection -** active le journal d'audit des tentatives de connexion à un serveur IRC. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception de messages instantanés. *Le Chat, l'ID de tous les participants MI, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'ID du participant local précède l'ID du participant à distance*. **Shadowing: Incoming Messages** - active la copie de réplication des messages instantanés reçus.

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus. **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.
Jabber	**Audit: Connection** - active le journal d'audit des tentatives de connexion à un serveur Jabber. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception des messages instantanés. *Le Chat, l'ID de tous les participants MI, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'ID du participant local précède l'ID du participant à distance*. **Shadowing: Incoming Messages** - active la copie de réplication des messages instantanés reçus. *Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus*. **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.
Mail.ru Agent	**Audit: Connection -** active le journal d'audit des tentatives de connexion au serveur Mail.ru Agent to the Mail.ru. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception des messages instantanés. *Le Chat, l'ID de tous les participants MI, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'ID du participant local précède l'ID du participant à distance*. **Shadowing: Incoming Messages** - active la copie de réplication des messages

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	instantanés reçus. *Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus*. **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.
SMTP	**Audit: Connection -** active le journal d'audit des tentatives de connexion à un serveur SMTP. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Outgoing Messages**, **Audit: Outgoing Files** - active le journal d'audit des tentatives d'envoi d'un email avec ou sans pièces jointes. *L'action Outgoing Message, l'adresse email de l'expéditeur et des destinataires, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'adresse de l'expéditeur précède l'adresse du destinataire (expéditeur=>destinataire1, destinataire2)*. **Shadowing: Outgoing Messages**, **Shadowing: Outgoing Files -** active le journal d'audit des emails envoyés avec ou sans pièces jointes. *Les copies de réplication des emails envoyés avec ou sans pièces jointes sont consignées dans le journal au format .eml. Vous pouvez ouvrir les fichiers .eml à l'aide de Microsoft Outlook Express, Windows Mail, et Mozilla Thunderbird*.
Social Networks (Réseaux Sociaux)	**Audit: Connection -** active le journal d'audit des tentatives de connexion à un site de réseau social. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Outgoing Messages -** active le journal d'audit des tentatives d'envoi de messages, commentaires, articles, etc. *L'action Outgoing Message et l'information suivante (<site_name>_<content_name>_<Recipient ID>) sont consignés dans le journal. Les ID des destinataires sont consignés dans le journal uniquement si les utilisateurs essaient d'envoyer des messages. Les ID des destinataires sont consignés sous forme de chiffres*. **Audit: Outgoing Files** - active le journal d'audit des tentatives de téléchargement d'un média et d'un fichier sur un site de réseau social. *L'action Outgoing File et l'information suivante (<site_name>_<content_name>_<Recipient ID>) sont consignés dans le journal*.

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	Shadowing: Outgoing Messages - active la copie de réplication des messages, commentaires, articles, etc, envoyés. *Les copies de réplication des messages, commentaires, etc. envoyés sont consignées dans le journal*. **Shadowing: Outgoing Files** - active la copie de réplication des fichiers téléchargés sur un site de réseau social. *Les copies de réplication des fichiers téléchargés sont consignées dans le journal*.
Telnet	**Audit: Connection -** active le journal d'audit des tentatives de connexion à un site Telnet. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*.
Web Mail	**Audit: Connection -** active le journal d'audit des tentatives d'accès à la messagerie Web. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal.* **Audit: Outgoing Messages**, **Audit: Outgoing Files -** active le journal d'audit des tentatives d'envoi d'un email avec ou sans pièces jointes. *L'action Outgoing Message, le nom du fournisseur de la messagerie Web (comme Yahoo, Gmail, Hotmail) l'adresse email de l'expéditeur et des destinataires, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'adresse de l'expéditeur précède l'adresse du destinataire (expéditeur=>destinataire1, destinataire2)*. **Shadowing: Outgoing Messages**, **Shadowing: Outgoing Files -** active le journal d'audit des emails envoyés avec ou sans pièces jointes. *Les copies de réplication des emails envoyés avec ou sans pièces jointes sont consignées dans le journal au format .eml. Vous pouvez ouvrir les fichiers .eml à l'aide de Microsoft Outlook Express, Windows Mail, et Mozilla Thunderbird.* **Remarque:** Les services de messagerie Web enregistrent automatiquement les brouillons des messages. DeviceLock gère l'enregistrement d'un brouillon comme l'envoi d'un message.
Windows Messenger	**Audit: Connection -** active le journal d'audit des tentatives de connexion au serveur Windows Messenger. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception des messages instantanés. *Le Chat, l'ID du participant local, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal*. **Shadowing: Incoming Messages** - active la copie de réplication des messages instantanés reçus.

PROTOCOLE	DROITS D'AUDIT ET DE RÉPLICATION
	Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus. **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.
Yahoo Messenger	**Audit: Connection -** active le journal d'audit des tentatives de connexion au serveur Yahoo Messenger. *La Connection, l'adresse IP avec le numéro du port, le nom de l'hôte et le nom du protocole sont consignés dans le journal. Si le rapprochement entre adresse IP et nom d'hôte échoue, le nom de l'hôte n'est pas consigné dans le journal*. **Audit: Incoming Messages**, **Outgoing Messages** - active le journal d'audit des tentatives d'envoi et de réception des messages instantanés. *Le Chat, l'ID de tous les participants MI, l'adresse IP avec le numéro du port et le nom de l'hôte sont consignés dans le journal. L'ID du participant local précède l'ID du participant à distance*. **Shadowing: Incoming Messages** - active la copie de réplication des messages instantanés reçus. *Les copies de réplication des messages instantanés reçus sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages reçus*. **Shadowing: Outgoing Messages** - active la copie de réplication des messages instantanés envoyés. *Les copies de réplication des messages instantanés envoyés sont consignées dans le journal au format .txt. Une copie de réplication des messages est consignée dans le journal après 30 minutes d'inactivité (soit 30 minutes après le dernier échange de la session de chat) ou si l'utilisateur abandonne la messagerie instantanée. Elle contient l'enregistrement exact de tous les messages envoyés*.

Remarque: Vous pouvez définir des règles d'audit et de réplication différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les règles d'audit et de réplication en ligne (Regular Profile) s'appliquent aux ordinateurs client qui fonctionnent en ligne. Les règles d'audit et de réplication hors ligne (Offline Profile) s'appliquent aux ordinateurs client qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des règles d'audit et de réplication hors ligne, reportez-vous au chapitre intitulé «Gestion des règles d'audit et de réplication hors ligne des protocoles.»

Vous pouvez configurer les règles d'audit et de réplication par défaut pour les deux types de profiles (Regular Profile et Offline Profile). Les règles par défaut s'appliquent aux groupes Users et Everyone. La table suivante contient les droits accordés à ces groupes par défaut.

GROUPE/ PROTOCOLE	USERS	EVERYONE
FTP	Audit: Connection Audit: Incoming Files Audit: Outgoing Files	Audit: Connection Audit: Incoming Files Audit: Outgoing Files
HTTP	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files
ICQ/AOL Messenger	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
IRC	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Jabber	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Mail.ru Agent	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
SMTP	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Social Networks	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Telnet	Audit: Connection	Audit: Connection
Web Mail	Audit: Connection Audit: Outgoing Messages	Audit: Connection Audit: Outgoing Messages

GROUPE/ PROTOCOLE	USERS	EVERYONE
	Audit: Outgoing Files	Audit: Outgoing Files
Windows Messenger	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Yahoo Messenger	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages

La gestion en ligne (regular) des règles d'audit et de réplication comprend les tâches suivantes:

- Définition et édition de règles d'audit et de réplication
- Révocation de règles d'audit et de réplication

Les règles d'audit et de réplication en ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les règles d'audit et de réplication ne sont pas définies pour le protocole.
Configured	Indique que les règles d'audit et de réplication sont définies pour le protocole.
No Audit	Indique une des situations suivantes: • Les droits d'audit ne sont pas définis pour tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du protocole. • Tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du protocole sont supprimés. • Le compte Everyone n'a ni droits d'audit ni droits de réplication et c'est le seul compte spécifié dans les règles d'audit et de réplication du protocole.

Définition et édition de règles d'audit et de réplication

Pour définir et éditer des règles d'audit et de réplication

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

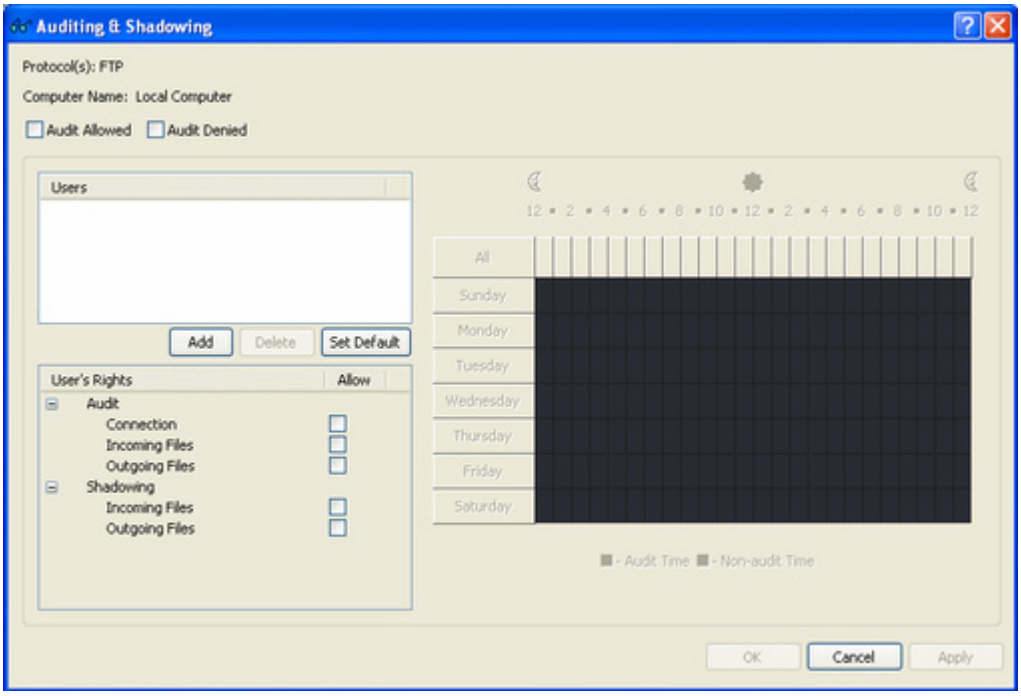
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles en ligne de chaque protocole dans la colonne Regular.
4. Dans le panneau de détails, procédez comme suit:
   - Cliquez droit sur le protocole pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur **Set Auditing & Shadowing**.
     - OU -
   - Sélectionnez le protocole pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur le bouton **Set Auditing & Shadowing** de la barre d'outils.
     - OU -
   - Double-cliquez sur le protocole pour lequel vous souhaitez définir ou éditer des règles.

   La boîte de dialogue Auditing & Shadowing apparaît.



5. Dans la boîte de dialogue **Auditing & Shadowing**, procédez comme suit:

ACTION	PROCEDURE
Définir des règles d'audit	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies

ACTION	PROCEDURE
et de réplication par défaut	d'accès à un protocole. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un protocole. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Set Default**. *Les règles d'audit et de réplication par défaut s'appliquent aux groupes Users et Everyone. Pour en savoir plus sur les droits d'audit et de réplication définis pour ces comptes par défaut, consultez le chapitre intitulé* «Gestion des règles d'audit et de réplication de protocoles.»
Définir des règles d'audit et de réplication pour un utilisateur ou un groupe supplémentaire	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies d'accès à un protocole. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un protocole. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît*. 3. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Auditing & Shadowing*. 4. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue **Auditing & Shadowing**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. 5. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Auditing & Shadowing**, cochez ou décochez la case **Allow** située en regard des droits appropriés. *Dans le panneau de droite de la boîte de dialogue Auditing & Shadowing, vous pouvez indiquer les jours et les horaires (par exemple, de 7h00 à 17h00 du lundi au vendredi) pendant lesquels les règles définies pour un utilisateur particulier s'appliquent ou non. Utilisez le bouton gauche de la souris et sélectionnez la période pendant laquelle la règle est appliquée (période d'audit). Utilisez le bouton droit de la souris et sélectionnez la période pendant laquelle la règle n'est pas appliquée (période de non audit)*.
Changer des règles d'audit et de réplication pour un utilisateur ou un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés.
Supprimer un utilisateur ou un groupe	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

ACTION	PROCEDURE
existant et les règles	*Quand vous supprimez un utilisateur ou un groupe, les règles associées à cet utilisateur ou groupe sont aussi supprimées*.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation de règles d'audit et de réplication

Si vous déployez des politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou DeviceLock Service Settings Editor, dans certaines situations vous pouvez empêcher l'application des règles d'audit et de réplication d'un protocole particulier ou de tous les protocoles à certains groupes d'ordinateurs client. Pour ce faire, vous devez redonner aux règles précédemment définies le statut non configuré. Tous les paramètres DeviceLock non définis sont ignorés par les ordinateurs clients.

Pour révoquer des règles d'audit et de réplication

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des règles d'audit et de réplication.
4. Dans le panneau de détails, cliquez droit sur le protocole dont vous voulez révoquer les règles, puis cliquez sur **Undefine**.

   Vous pouvez révoquer les règles de plusieurs protocoles en même temps. Pour ce faire, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine**.

Gestion de la liste blanche de protocoles

La liste blanche de protocoles vous permet d'accorder des permissions sélectives aux communications réseau pour les protocoles pris en charge, indépendamment des paramètres de blocage de protocoles existants. Les listes blanches sont plus efficaces dans

les scénarios de «moindre privilège», lorsque tous les protocoles sont bloqués et qu'elles autorisent uniquement ceux nécessaires à l'accomplissement des tâches quotidiennes des employés.

Par exemple, supposons que l'accès aux protocoles SMTP et Web Mail soit refusé à tous les utilisateurs, et que vous utilisiez la liste blanche pour permettre à certains utilisateurs d'envoyer des emails à des adresses spécifiques afin qu'ils puissent exécuter leurs tâches. En appliquant ces politiques de sécurité, vous pouvez réduire les éventuels risques de fuite de données, vol et mauvaise utilisation.

Remarque: Aucun audit ni réplication n'a lieu pour les transferts de données autorisés par la liste blanche des protocoles pendant l'audit des connexions en liste blanche.

La liste blanche comporte les règles associées aux protocoles. Chaque règle détermine les utilisateurs ou les groupes à qui elle s'applique, ainsi que l'ensemble des paramètres qui lui sont associés. Ces paramètres se divisent en deux catégories:

- Paramètres généraux applicables à tous les protocoles
- Paramètres propres à un protocole

La table suivante indique les paramètres généraux pour une règle de la liste blanche.

PARAMÈTRE	DESCRIPTION
Protocol	Indique la règle applicable au protocole.
Description	Indique le nom de la règle.

La table suivante indique les paramètres propres à un protocole pour une règle de la liste blanche.

PARAMÈTRE	DESCRIPTION
Hosts:	S'applique aux protocoles FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, Telnet, Windows Messenger et Yahoo Messenger Indique une liste d'hôtes autorisés pour cette règle. Si cette liste est définie, ces hôtes ne seront pas bloqués. Les hôtes peuvent être spécifiés dans l'un des formats suivants: • Nom DNS (par exemple, **www.example.com**). Vous pouvez utiliser des caractères joker comme l'astérisque (*) dans les noms DNS (par exemple, ***.example.com** indique que le nom de l'hôte peut être tout serveur ayant cette terminaison spécifique). **Attention:** Le fait d'ajouter des noms d'hôtes avec des jokers à la liste blanche pour tous les protocoles à l'exception du protocole HTTP ne garantit pas que la règle de la liste blanche fonctionnera comme prévu. Étant donné que DeviceLock utilise le fichier local Hosts pour le rapprochement avec le nom d'hôte, un utilisateur mal intentionné ayant des droits d'administrateur local

PARAMÈTRE	DESCRIPTION
	peut modifier le fichier Hosts pour contourner les politiques de sécurité DeviceLock. Par exemple, si la liste blanche autorise l'accès http à gmail.com, un utilisateur mal intentionné avec des droits d'administrateur local peut accéder au site non autorisé www.ru en ajoutant «**194.87.0.50 gmail.com**» au fichier Hosts. Pour réduire les risques en matière de sécurité, nous vous conseillons de spécifier les adresses IP plutôt que les noms d'hôte. • Adresse IP (par exemple, **12.13.14.15**). Vous pouvez spécifier une plage d'adresses IP séparées par tiret (-) (par exemple, **12.13.14.18-12.13.14.28**). Vous pouvez aussi spécifier un masque de sous-réseau pour l'adresse IP à l'aide du format suivant*: Largeur en bits de l'adresse IP/masque de sous-réseau* (par exemple, **3.4.5.6/16**). Les hôtes multiples doivent être séparés par des virgules (,) ou des points-virgules (;). Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée. Vous pouvez spécifier plusieurs hôtes dans les formats décrits ci-dessus (par exemple, www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28). **Remarque:** Quand vous ajoutez des hôtes à la liste blanche, tenez compte des points suivants: Si les objets (images, scripts, vidéo, fichiers Flash, ActiveX, etc.) d'une page Web sont téléchargés à partir d'autres hôtes, vous devez ajouter ces hôtes à la liste blanche pour charger correctement la page Web. Si vous spécifiez les hôtes et non les ports, l'accès aux hôtes peut se faire via n'importe quel port disponible. Une application avec un certificat SSL intégré (par exemple, Microsoft Office Communicator, Dropbox, iTunes, module de synchronisation des contacts de Google, etc.) ne peut pas se connecter à son serveur quand le module NetworkLock est actif. Le module NetworkLock est actif quand les paramètres des protocoles sont définis. Pour résoudre ce problème, ajoutez l'hôte de serveur à la liste blanche du protocole SSL. Vous pouvez utiliser TcpView pour voir l'hôte de serveur. Lorsqu'on met en liste blanche un hôte de serveur, tout le trafic SSL entre une application et le serveur spécifié contourne le contrôle d'accès, l'audit, la copie de réplication et le filtrage de données.
Ports:	S'applique aux protocoles FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, Telnet, Windows Messenger et Yahoo Messenger. Indique le ou les ports à ouvrir pour cette règle. Si cette liste est définie, ces ports ne seront pas bloqués. Vous pouvez spécifier un seul port ou une plage inclusive de ports séparés par des tirets (-). Par exemple, pour ouvrir le port 25, spécifiez **25**. Pour ouvrir les ports 5000 à 5020 inclus, spécifiez **5000-5020**. Les ports multiples ou les plages de ports doivent être séparés par des virgules (,) ou des points-virgules (;). Par exemple, **25, 36; 8080, 5000-5020**. Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée. **Remarque:** Si vous spécifiez les ports mais pas les hôtes, les utilisateurs peuvent

PARAMÈTRE	DESCRIPTION
	accéder à tous les hôtes disponibles via les ports spécifiés.
SSL	S'applique aux protocoles FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, SMTP, et Web Mail. Definit les options SSL. Les options SSL suivantes sont disponibles: • **Allowed** Autorise les connexions SSL. • **Denied** N'autorise pas les connexions SSL. • **Required** Toutes les connexions doivent utiliser SSL.
Local sender ID(s):	S'applique aux protocoles ICQ/AOL Messenger, Jabber, Mail.ru Agent, Windows Messenger et Yahoo Messenger. Indique une liste d'identifiants pour les utilisateurs locaux qui sont autorisés à envoyer des messages instantanés. Si cette liste est définie, les messages instantanés de ces utilisateurs ne seront pas bloqués. Les utilisateurs d'ICQ/AOL Messenger sont identifiés par un numéro dit «UIN» (par exemple, **111222, 23232323**). Les utilisateurs de Jabber sont identifiés par des ID Jabber aux formats suivants: **user@example.com**. Les utilisateurs de Mail.ru Agent sont identifiés par les adresses mail.ru e-mail aux formats suivants: **user@mail.ru**. Les utilisateurs de Windows Messenger sont identifiés par les adresses d'email aux formats suivants: **user@example.com**. Les utilisateurs de Yahoo Messenger sont identifiés par un des types d'ID utilisateur suivants: • **Yahoo! ID** (<nom d'utilisateur> ou <nom d'utilisateur>@yahoo.com) • **Rocketmail** (<nom d'utilisateur>@rocketmail.com) • **Ymail** (<nom d'utilisateur>@ymail.com) Les différents identifiants des utilisateurs doivent être séparés par des virgules (,) ou des points-virgules (;). Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée.
Remote recipient ID(s):	S'applique aux protocoles ICQ/AOL Messenger, Jabber, Mail.ru Agent et Yahoo Messenger. Indique une liste d'identifiants pour les utilisateurs à distance qui sont autorisés à recevoir des messages instantanés. Si cette liste est définie, les messages instantanés de ces utilisateurs ne seront pas bloqués. Les utilisateurs d'ICQ/AOL Messenger sont identifiés par un numéro dit «UIN» (par exemple, **111222, 23232323**). Les utilisateurs de Jabber sont identifiés par des ID Jabber aux formats suivants: **user@example.com**. Les utilisateurs de Mail.ru Agent sont identifiés par les adresses mail.ru e-mail aux formats suivants: **user@mail.ru**. Les utilisateurs de Windows Messenger sont identifiés par les adresses d'email aux formats suivants: **user@example.com**. Les utilisateurs de Yahoo Messenger sont identifiés par un des types d'ID utilisateur suivants:

PARAMÈTRE	DESCRIPTION
	• **Yahoo! ID** (<nom d'utilisateur> ou <nom d'utilisateur>@yahoo.com) • **Rocketmail** (<nom d'utilisateur>@rocketmail.com) • **Ymail** (<nom d'utilisateur>@ymail.com) Les différents identifiants des utilisateurs doivent être séparés par des virgules (,) ou des points-virgules (;). Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée.
Local sender Email(s):	S'applique aux protocoles SMTP et Web Mail. Indique une liste d'expéditeurs d'emails autorisés pour cette règle. Si cette liste est définie, les emails de ces expéditeurs ne seront pas bloqués. Utilisez les formats suivants pour l'adresse de l'expéditeur: *user@domain.com*. Vous pouvez utiliser un caractère joker comme l'astérisque (*) pour spécifier un groupe de destinataires. Vous pouvez ajouter l'astérisque avant ou après le symbole (@) de l'adresse email. Par exemple, pour autoriser l'acheminement des emails de tous les utilisateurs vers un domaine, saisissez ***@domain.com**. Les différentes adresses email doivent être séparées par des virgules (,) ou des points-virgules (;). Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée. **Remarque:** Quand vous ajoutez des expéditeurs et des destinataires à la liste blanche de la messagerie Web, tenez compte des points suivants: Les messages envoyés à partir de l'application Webmail sont gardés dans le dossier «Sent Items» et peuvent être acheminés vers n'importe quelle adresse à partir de n'importe quel ordinateur.
Remote recipient Email(s):	S'applique aux protocoles SMTP et Web Mail. Indique une liste de destinataires d'emails autorisés pour cette règle. Si cette liste est définie, les emails de ces destinataires ne seront pas bloqués. Utilisez les formats suivants pour l'adresse du destinataire: *user@domain.com*. Vous pouvez utiliser un caractère joker comme l'astérisque (*) pour spécifier un groupe de destinataires. Vous pouvez ajouter l'astérisque avant ou après le symbole (@) de l'adresse email. Par exemple, pour autoriser l'acheminement des emails de tous les utilisateurs vers un domaine, saisissez ***@domain.com**. Les différentes adresses email doivent être séparées par des virgules (,) ou des points-virgules (;). Vous pouvez aussi appuyer sur la touche ENTRÉE après chaque entrée.
Social Networks	S'applique au protocole des réseaux sociaux. Indique une liste de sites de réseaux sociaux autorisés dans le cadre de cette règle. Si cette liste est définie, ces sites de réseaux sociaux ne seront pas bloqués. Les sites de réseaux sociaux suivants sont pris en charge: Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING.
Web Mail Services	S'applique au protocole de Messagerie. Indique une liste de services de messagerie autorisés dans le cadre de cette règle. Si cette liste est définie, les emails envoyés au moyen de ces services de messagerie ne seront pas bloqués. Les services de messagerie suivants sont pris en charge: AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, et Yandex Mail.

Remarque: Vous pouvez définir des listes blanches de protocoles différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. La liste blanche de protocoles en ligne (Regular Profile) s'applique aux ordinateurs clients qui fonctionnent en ligne. La liste blanche de protocoles hors ligne (Offline Profile) s'applique aux ordinateurs clients qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des protocoles hors ligne, reportez-vous au chapitre intitulé «Gestion de la liste blanche de protocoles hors ligne.»

La gestion de la liste blanche de protocoles en ligne (regular) comprend les tâches suivantes:

- Définition de la liste blanche de protocoles
- Édition de la liste blanche de protocoles
- Copie des règles de la liste blanche de protocoles
- Exportation et importation de la liste blanche de protocoles
- Révocation de la liste blanche de protocoles
- Suppression des règles de la liste blanche de protocoles

Définition de la liste blanche de protocoles

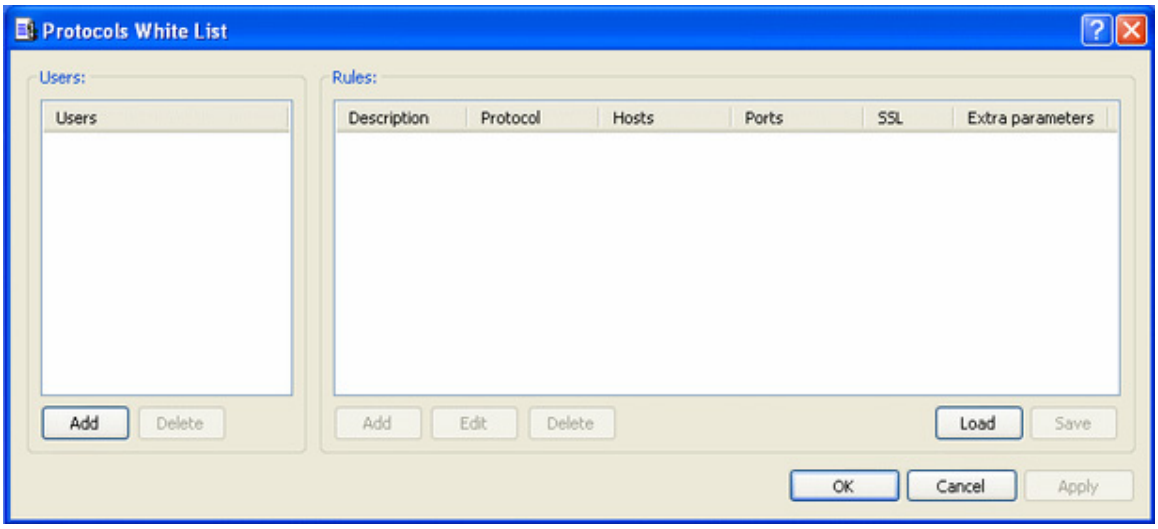
Pour définir la liste blanche de protocoles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Protocols White List apparaît.



4. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la liste blanche de protocoles, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau gauche de la boîte de dialogue Protocols White List.

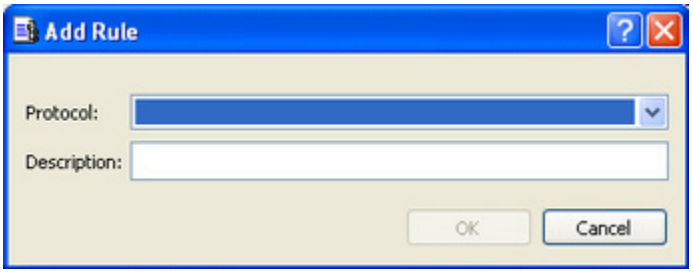
   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, puis cliquez sur **Delete**.

6. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, sélectionnez l'utilisateur ou le groupe souhaité.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, cliquez sur **Add**.

   La boîte de dialogue Add Rule apparaît.



8. Dans la boîte de dialogue **Add Rule**, spécifiez les paramètres généraux et les paramètres propres au protocole pour cette règle. Pour spécifier les paramètres généraux, procédez comme suit:

- Pour spécifier le protocole, dans le champ **Protocol:** cliquez sur le protocole de votre choix.
- Pour spécifier le nom de la règle, saisissez un nom dans le champ **Description**.

Pour spécifier les paramètres propres au protocole, procédez comme suit:

- Pour spécifier les hôtes, dans le champ **Hosts:** saisissez les noms ou les adresses IP des hôtes, séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des hôtes, reportez-vous à la description du paramètre Hôtes qui précède.
- Pour spécifier les ports, dans le champ **Ports:** saisissez les numéros de port séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des ports, reportez-vous à la description du paramètre Ports qui précède.
- Pour configurer les options SSL, dans le champ **SSL**, cliquez sur l'une ou l'autre des options suivantes: **Allowed** (autorise les connexions SSL), **Denied** (n'autorise pas les connexions SSL), ou **Required** (toutes les connexions doivent utiliser SSL).
- Pour spécifier l'ID(s) de l'expéditeur local MI, dans le champ **Local sender ID(s):** saisissez les identifiants d'utilisateur, séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des identifiants de l'utilisateur, reportez-vous à la description du paramètre ID(s) d'expéditeur local qui précède.
- Pour spécifier le ou les ID(s) de destinataire distant MI, dans le champ **Remote recipient ID(s):** saisissez les identifiants d'utilisateur séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des identifiants d'utilisateur, reportez-vous à la description du paramètre ID(s) de destinataire distant qui précède.
- Pour spécifier les expéditeurs d'emails, dans le champ **Local sender Email(s):** saisissez les adresses d'expéditeur séparées par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des adresses de l'expéditeur, reportez-vous à la description du paramètre Email(s) d'expéditeur local qui précède.
- Pour spécifier les destinataires d'emails, dans le champ **Remote recipient Email(s):** saisissez les adresses de destinataire séparées par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des adresses de destinataire, reportez-vous à la description du paramètre Email(s) de destinataire distant qui précède.
- Pour spécifier les sites de réseaux sociaux, cochez ou décochez les cases appropriées dans le champ **Social Networks:** Pour en savoir plus, reportez-vous à la description du paramètre Réseaux sociaux qui précède.
- Pour spécifier les services de messagerie Web, cochez ou décochez les cases appropriées dans le champ **Web Mail Services:** Pour en savoir plus, reportez-vous à la description du paramètre Services de messagerie qui précède.

9. Cliquez sur **OK**.

   La règle ainsi créée figure dans le champ Rules du panneau droit de la boîte de dialogue Protocols White List.

10. Cliquez sur **OK** ou sur **Apply**.

Les utilisateurs ou les groupes auxquels s'applique la règle de la liste blanche sont affichés dans le champ White List de l'arborescence de console.

Si vous sélectionnez un utilisateur ou un groupe auquel la règle de la liste blanche s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

- **Protocol** La règle applicable au protocole.
- **Description** Le nom de la règle.
- **Hosts** Indique les hôtes autorisés pour cette règle.
- **Ports** Indique les ports autorisés pour cette règle.
- **SSL** Indique l'option SSL sélectionnée. Valeurs possibles: **Allowed** (autorise les connexions SSL), **Denied** (n'autorise pas les connexions SSL), et **Required** (toutes les connexions doivent utiliser SSL).
- **Extra parameters** Indique les paramètres supplémentaires propres au protocole pour cette règle. Ces paramètres incluent: **From** (indique les identifiants de l'expéditeur pour la messagerie instantanée et les adresses email de l'expéditeur pour la messagerie Web) et **To** (indique les identifiants du destinataire pour la messagerie instantanée et les adresses email du destinataire pour la messagerie Web).
- **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs clients qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs clients qui travaillent hors ligne.

  Vous pouvez définir des listes blanches de protocoles différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur le mode de définition de la liste blanche de protocoles hors ligne, reportez-vous au chapitre intitulé «Gestion de la liste blanche de protocoles hors ligne.»

Édition de liste blanche de protocoles

Vous pouvez modifier les valeurs des paramètres spécifiées pour une règle de liste blanche à tout instant.

Pour modifier une règle de liste blanche

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquer droit sur **White List**, cliquer sur **Manage**, puis faire la chose suivante:

a) Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.

Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans l'option Rules du panneau droit de la boîte de dialogue.

b) Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.

- OU -

Cliquez droit sur la règle, puis cliquez sur **Edit**.

- OU -

Dans **Protocols**, développez **White List**, puis procédez comme suit:

a) Dans **White List**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.

Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans le panneau de détails.

b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.

- OU -

Dans le panneau de détails, double-cliquez sur la règle que vous souhaitez modifier.

La boîte de dialogue Edit Rule apparaît.

4. Dans la boîte de dialogue **Edit Rule**, modifiez les paramètres des règles en fonction de vos besoins.
5. Cliques sur **OK** pour valider les modifications.

Copie des règles de la liste blanche de protocoles

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles existantes de la liste blanche de protocoles.

Pour copier une règle de liste blanche

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Manage**.
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Manage** de la barre d'outils.

   La boîte de dialogue Protocols White List apparaît.
4. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle que vous souhaitez copier.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans l'option Rules du panneau droit de la boîte de dialogue.
5. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, cliquez droit sur la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

   La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

   Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Lorsque vous utilisez la combinaison de touches CTRL+X pour couper la règle, la règle ne sera coupée qu'une fois copiée.
6. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.
7. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes auxquels s'applique la règle que vous souhaitez copier, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau gauche de la boîte de dialogue Protocols White List.
8. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez appliquer la règle ainsi copiée.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
9. Dans le panneau droit de la boîte de dialogue **Protocols White List**, cliquez droit sur le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée figure dans le champ Rules du panneau droit de la boîte de dialogue Protocols White List.
10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de liste blanche de protocoles

Vous pouvez exporter toutes vos règles de la liste blanche de protocoles en cours dans un fichier .pwl puis importer et utiliser celui-ci sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter la liste blanche de protocoles

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Save.**
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Save** de la barre d'outils.
     - OU -
   - Développez **White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Save**.
     - OU -
   - Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur la règle de liste blanche, puis cliquez sur **Save**.
     - OU –
   - Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur l'option **Save** de la barre d'outils.
     - OU -
   - Cliquez droit sur **White List**, puis cliquez sur **Manage**. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, cliquez sur **Save**.

   La boîte de dialogue Save As apparaît.
4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .pwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

Lorsque vous exportez la liste blanche de protocoles, celle-ci est sauvegardée dans un fichier doté d'une extension .pwl.

Pour importer la liste blanche de protocoles

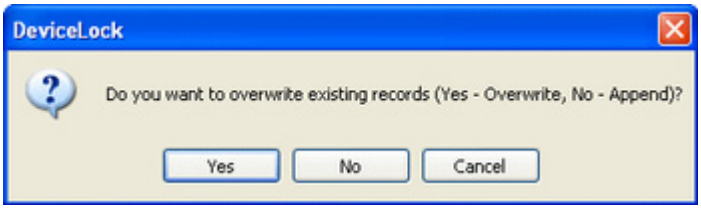
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Load**.
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Load** de la barre d'outils.
     - OU -
   - Développez **White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Load**.
     - OU -
   - Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur la règle de liste blanche, puis cliquez sur **Load**.
     - OU -
   - Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur l'option **Load** de la barre d'outils.
     - OU -
   - Cliquez droit sur **White List**, puis cliquez sur **Manage**. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, cliquez sur **Load**.

   La boîte de dialogue Open apparaît.
4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Si la liste blanche de protocoles est déjà définie et que vous choisissez d'importer une nouvelle liste blanche, le champ de message suivant s'affiche.



Dans le champ de message, cliquez sur **Yes** pour écraser la liste blanche existante. Cliquez sur **No** pour ajouter une nouvelle liste blanche à la liste blanche existante.

Révocation de liste blanche de protocoles

Si vous déployez des politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou DeviceLock Service Settings Editor, dans certaines situations vous pouvez souhaiter empêcher l'application de la liste blanche de protocoles à un groupe d'ordinateurs clients donné. Pour ce faire, vous devez redonner à la liste blanche précédemment définie le statut non configuré. Tous les paramètres DeviceLock non définis sont ignorés par les ordinateurs clients.

Pour révoquer la liste blanche de protocoles

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **White List** puis cliquez sur **Undefine**.

Suppression de règles de liste blanche de protocoles

Vous pouvez supprimer les règles de liste blanche individuelles qui ne sont plus nécessaires.

Pour supprimer une règle de liste blanche

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:

- Développez **White List**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.
  Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.
  - OU -
- Développez **White List**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.
  - OU -
- Cliquez droit sur **White List**, puis cliquez sur **Manage**. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.

Gestion des paramètres de sécurité pour les protocoles

Vous pouvez définir des paramètres de sécurité supplémentaires qui affectent les autorisations et les règles d'audit pour les protocoles.

DeviceLock accepte les paramètres additionnels de sécurité suivants:

- **Block unrecognized outgoing SSL traffic**: activé, ce paramètre permet au DeviceLock Service d'auditer et de bloquer tout le trafic SSL sortant non reconnu. Sinon, même si les protocoles sont verrouillés, le trafic SSL sortant non reconnu n'est pas bloqué et ne fait pas l'objet d'un audit.
- **Block IP addresses in URL:** activé, ce paramètre permet au DeviceLock Service de bloquer tous les URL contenant l'adresse IP d'hôte lorsque les utilisateurs disposent d'autorisations «allow access» (permettre l'accès) à un protocole. Utiliser ce paramètre pour bloquer l'accès aux sites (Facebook, par exemple) auxquels il est possible d'accéder à l'aide d'une adresse IP. Ce paramètre s'applique aux protocoles suivants: HTTP, réseaux sociaux et messagerie Internet. Par défaut, ce paramètre est désactivé.
  L'audit et la réplication des URL contenant l'adresse IP d'hôte ont lieu au niveau http. Si l'option Block IP addresses in URL (Refuser les adresses IP dans l'URL) est désactivée, mais que les utilisateurs ont des autorisations «deny access» (refuser l'accès) à un protocole, tous les URL contenant l'adresse IP d'hôte sont également bloqués.

Remarque: Si l'option **Block IP addresses in URL** est désactivée et que des adresses IP d'hôte spécifiques sont autorisées par la liste blanche des protocoles, ces adresses IP ne seront pas bloquées. Les paramètres de liste blanche des protocoles sont prioritaires par rapport aux paramètres de sécurités des protocoles.

Remarque: Vous pouvez définir des paramètres de sécurité différents selon qu'ils s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Les paramètres de sécurité en ligne (Regular Profile) s'appliquent aux ordinateurs clients qui fonctionnent en ligne. Les paramètres de sécurité hors ligne (Offline Profile) s'appliquent aux ordinateurs clients qui fonctionnent hors ligne. Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client. Pour en savoir plus sur les politiques hors ligne de DeviceLock, reportez-vous au chapitre intitulé «Politiques de sécurité de DeviceLock (Offline Profile).» Pour en savoir plus sur le mode de définition des paramètres de sécurité hors ligne, reportez-vous au chapitre intitulé «Gestion des paramètres de sécurité hors ligne des protocoles.»

La gestion des paramètres de sécurité (regular) comprend les tâches suivantes:

- Définition et modification de paramètres de sécurité
- Révocation de paramètres de sécurité

Les paramètres de sécurité en ligne de protocoles peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les paramètres de sécurité ne sont pas définis pour les protocoles.
Enabled	Indique que les paramètres de sécurité sont activés pour les protocoles.
Disabled	Indique que les paramètres de sécurité sont désactivés pour les protocoles.

Définition et modification de paramètres de sécurité

Pour définir et modifier les paramètres de sécurité

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:

- Sélectionnez **Security Settings**. Dans le panneau de détails, cliquez droit sur le paramètre de sécurité, puis cliquez sur **Enable** ou **Disable**.

  Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.

  - OU -
- Cliquez droit sur **Security Settings**, puis cliquez sur **Manage**. Dans la boîte de dialogue **Security Settings** qui s'ouvre, cochez ou décochez la case appropriée, puis cliquez sur **OK**.

  Pour ouvrir la boîte de dialogue Security Settings, vous pouvez aussi sélectionner Security Settings, puis cliquer sur l'option Manage *de la boîte d'outils.*

Révocation de paramètres de sécurité

Si vous déployez des politiques DeviceLock à l'aide de DeviceLock Group Policy Manager ou DeviceLock Service Settings Editor, dans certaines situations vous pouvez souhaiter empêcher l'application de certains paramètres de sécurité définis pour les protocoles à un groupe d'ordinateurs clients donné. Pour ce faire, vous devez redonner aux paramètres de sécurité précédemment définis le statut non configuré. Tous les paramètres DeviceLock non définis sont ignorés par les ordinateurs clients.

Pour révoquer des paramètres de sécurité

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Service**, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Security Settings**.

   Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
4. Dans le panneau de détails, cliquez droit sur le paramètre de sécurité à révoquer, puis cliquez sur **Undefine**.

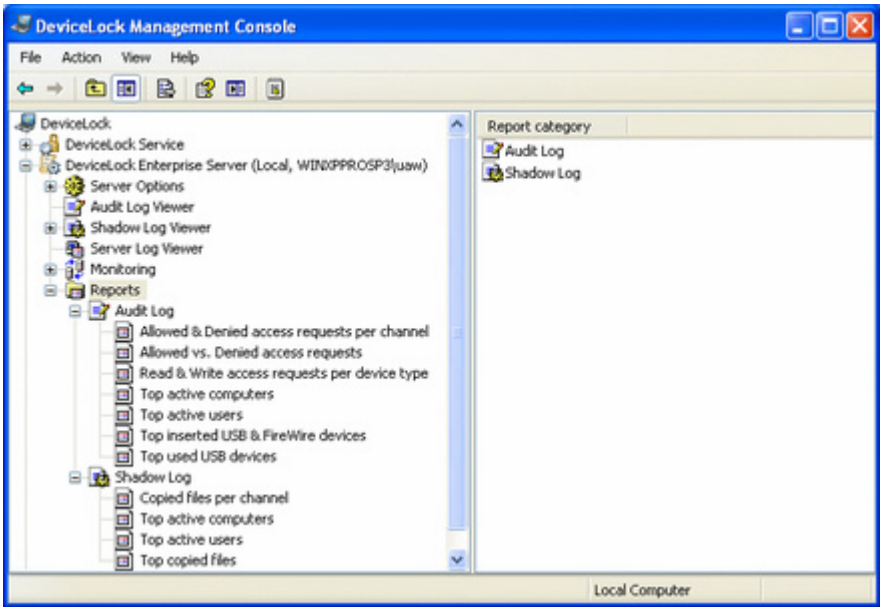
Rapports DeviceLock

DeviceLock permet de créer des rapports à l'aide des données de journaux stockées sur le DeviceLock Enterprise Server. Utilisez des rapports pour arranger et afficher des données statistiques sur les activités relatives au périphérique et aux protocoles d'un utilisateur sur un fichier séparer. Lors de la création d'un rapport, vous pouvez définir des paramètres permettant de filtrer les données et d'afficher les informations qui vous intéressent. Par exemple, vous pouvez préciser les dates de début et de fin, ainsi que la partie de la période de rapport pour laquelle les données sont affichées.

Les rapports peuvent être créés, envoyés automatiquement à votre attention par e-mail, stockés, exportés dans différents formats et partagés avec autrui. La création des rapports a lieu à l'aide de la DeviceLock Management Console.

Catégories et types de rapports

DeviceLock est livré avec une série de modèles de rapports prédéfinis que vous pouvez utiliser pour créer de nouveaux rapports. Ces modèles prédéfinis figurent dans l'arborescence, sous **DeviceLock Enterprise Server**, **Reports**.



Remarque: Vous ne pouvez créer que les rapports qui s'appuient sur les modèles prédéfinis. Vous ne pouvez ni modifier les modèles de rapports prédéfinis, ni créer vos propres modèles de rapports (personnalisés).

Il existe deux catégories de modèles de rapports:

- Les Audit Log reports (rapports de journaux d'audit)
- Les Shadow Log reports (rapports de journaux de réplication)

Les types de rapports disponibles dans chaque catégorie sont décrits ci-dessous.

Remarque: Lorsque vous mettez à niveau DeviceLock version 7.0, les rapports précédemment générés sont automatiquement mis à jour avec le même nom. Les demandes d'accès autorisées et refusées par type de périphérique deviennent les demandes d'accès autorisées et refusées par canal. Les demandes d'accès au périphérique autorisées vs. Refusées deviennent les demandes d'accès autorisées vs. refusées. Les fichiers copiés par type de périphérique deviennent les fichiers copiés par canal.

Audit Log Reports

Les Audit Log reports sont des rapports qui utilisent les fichiers de journaux d'audit du DeviceLock Enterprise Server en tant que source de données. Le tableau suivant contient un résumé des types de rapports disponibles dans cette catégorie.

TYPE DE RAPPORT	DESCRIPTION
Allowed & Denied access requests per channel	Ce rapport montre le nombre de demandes d'accès autorisées et refusées par canal de transmission de données (périphériques et/ou protocoles). Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **User(s):** Indique les utilisateurs concernés par le rapport. • **Channel(s):** montre les canaux de transmission de données indiquées pour le rapport. Les options disponibles sont les suivantes: **tous les périphériques**, **tous les protocoles**, et **tous les périphériques et protocoles**. La section Résultats de rapport comporte un tableau et un graphique avec les résultats détaillés du rapport. Ce tableau comporte les colonnes suivantes: • **Channel** montre un canal de transmission de données. • **Allowed** Indique le nombre de demandes d'accès autorisées. • **Denied** Indique le nombre de demandes d'accès refusées.
Allowed vs. Denied access requests	Ce rapport montre le nombre total de demandes d'accès autorisées et refusées par canal de transmission de données (périphériques et/ou protocoles). Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport.

TYPE DE RAPPORT	DESCRIPTION
	La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **User(s):** Indique les utilisateurs concernés par le rapport. • **Channel(s):** montre les canaux de transmission de données indiquées pour le rapport. Les options disponibles sont les suivantes: **tous les périphériques**, **tous les protocoles**, et **tous les périphériques et protocoles**. La section Résultats de rapport comporte un tableau et un graphique en gâteau avec les résultats détaillés du rapport. Ce tableau comporte les lignes suivantes: • **Allowed** Indique le nombre total de demandes d'accès autorisées et le pourcentage qu'elles représentent. • **Denied** Indique le nombre total de demandes d'accès refusées et le pourcentage qu'elles représentent. • **Total** Indique le nombre total de toutes les demandes d'accès et le pourcentage qu'elles représentent. Le graphique en gâteau présente les résultats du rapport sous forme de pourcentages.
Read & Write access requests per device type	Ce rapport indique le nombre de demandes d'accès en lecture et en écriture par type de périphériques. Seules y figurent les données relatives aux périphériques de types Floppy, iPhone, Removable, Hard disk, DVD/CD-ROM, Tape, Windows Mobile, et Palm. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Access Type(s):** Indique les types d'événements concernés par le rapport. • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **User(s):** Indique les utilisateurs concernés par le rapport. La section Résultats de rapport comporte un tableau et un graphique avec les résultats détaillés du rapport. Ce tableau comporte les colonnes suivantes: • **Device Type** Indique le type de périphérique • **Read** Indique le nombre de demandes d'accès en lecture seule. • **Write** Indique le nombre de demandes d'accès en écriture seule.

TYPE DE RAPPORT	DESCRIPTION
	Ce tableau comporte aussi une ligne **Total** avec un résumé de toutes les valeurs figurant dans les colonnes **Read** et **Write**.
Top active computers	Ce rapport indique les ordinateurs les plus souvent utilisés, triés en fonction du nombre de demandes d'accès autorisées et refusées. Par défaut, il comporte une liste des 10 premiers ordinateurs mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Channel(s):** montre les types de périphériques et/ou les protocoles spécifiés pour le rapport. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) premiers ordinateurs par nombre d'accès autorisés. Le tableau 2 comporte une liste des N (où N est un nombre entier) premiers ordinateurs par nombre d'accès refusés. Ces tableaux comportent les colonnes suivantes: • **Computer Name** Indique le nom de l'ordinateur • **Access Count** indique le nombre de demandes d'accès. Les valeurs de cette colonne sont triées par ordre décroissant.
Top active users	Ce rapport indique les utilisateurs les plus actifs, triés en fonction du nombre de demandes d'accès autorisées et refusées envoyé par chaque utilisateur. Par défaut, il comporte une liste des 10 premiers utilisateurs mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Channel(s):** montre les types de périphériques et/ou les protocoles spécifiés

TYPE DE RAPPORT	DESCRIPTION
	pour le rapport. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) premiers utilisateurs disposant d'une autorisation d'accès. Le tableau 2 comporte une liste des N (où N est un nombre entier) premiers utilisateurs à qui l'accès a été refusé. Ces tableaux comportent les colonnes suivantes: • **User Name** Indique le nom de l'utilisateur • **Access Count** indique le nombre de demandes d'accès. Les valeurs de cette colonne sont triées par ordre décroissant.
Top inserted USB & FireWire devices	Ce rapport indique les périphériques USB et FireWire les plus fréquemment introduits, triés par nombre d'insertions. Par défaut, il comporte une liste des 10 premiers périphériques mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Users(s):** Indique les utilisateurs concernés par le rapport. La section Résultats de rapport contient un tableau avec les résultats détaillés du rapport. Ce tableau comporte les colonnes suivantes: • **Device Name** Indique le nom de périphérique • **Insert Count** Indique le nombre d'insertions. Les valeurs de cette colonne sont triées par ordre décroissant.
Top used USB devices	Ce rapport indique les périphériques USB les plus souvent utilisés, triés en fonction du nombre de demandes d'accès autorisées et refusées. Par défaut, il comporte une liste des 10 premiers périphériques mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise*

TYPE DE RAPPORT	DESCRIPTION
	Server est exécuté. • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Users(s):** Indique les utilisateurs concernés par le rapport. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) principaux périphériques USB disposant d'une autorisation d'accès. Le tableau 2 comporte une liste des N (où N est un nombre entier) principaux périphériques USB à qui l'accès a été refusé. Ces tableaux comportent les colonnes suivantes: • **Device Name** Indique le nom de périphérique • **Access Count** Indique le nombre de demandes d'accès. Les valeurs de cette colonne sont triées par ordre décroissant.

Shadow Log Reports

Les Shadow Log reports sont des rapports qui utilisent les fichiers de journaux de réplication du DeviceLock Enterprise Server en tant que source de données. Tous ces rapports contiennent les données combinées du journal de réplication et du journal de réplication supprimé. Le tableau suivant contient un résumé des types de rapports disponibles dans cette catégorie.

TYPE DE RAPPORT	DESCRIPTION
Copied files per channel	Ce rapport montre les statistiques des fichiers copiés par canal de transmission de données (périphériques et/ou protocoles). Les informations statistiques sur les fichiers copiés sont triées en fonction du nombre de fichiers copiés et de la taille totale de tous les fichiers copiés. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Users(s):** Indique les utilisateurs concernés par le rapport. • **File Name:** Indique les fichiers concernés par le rapport en question. • **Channel(s):** montre les canaux de transmission de données indiquées pour le rapport. Les options disponibles sont les suivantes: **tous les périphériques**, **tous les protocoles**, et **tous les périphériques et protocoles**. La section Résultats de rapport comporte deux tableaux et deux graphiques en

TYPE DE RAPPORT	DESCRIPTION
	gâteau avec les résultats détaillés du rapport. Le Tableau 1 montre le nombre de fichiers copiés pour chaque canal de transmission de données. Il comporte les colonnes suivantes: • **Channel** montre un canal de transmission de données. • **Number of Files** Indique le nombre de fichiers copiés. Le tableau 1 comporte aussi une ligne intitulée **Total** avec la somme de toutes les valeurs de la colonne **Number of Files**. Le Tableau 2 montre la taille totale des fichiers copiés pour chaque canal de transmission de données. Il comporte les colonnes suivantes: • **Channel** montre un canal de transmission de données. • **Data Size** Indique la taille totale de tous les fichiers copiés. Ce tableau comporte aussi une ligne **Total** avec la somme de toutes les valeurs figurant dans la colonne **Data Size**. Chaque tableau est suivi d'un graphique en gâteau qui présente les résultats de rapport en pourcentages.
Top active computers	Ce rapport indique les ordinateurs les plus souvent utilisés, triés en fonction du nombre de fichiers copiés et de la taille totale de tous les fichiers copiés. Par défaut, il comporte une liste des 10 premiers ordinateurs mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté.* • **Channel(s):** montre les types de périphériques et/ou les protocoles spécifiés pour le rapport. • **File Name:** Indique les fichiers concernés par le rapport en question. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) premiers ordinateurs par nombre de fichiers copiés. Il comporte les colonnes suivantes: • **Computer Name** Indique le nom de l'ordinateur • **Number of Files** Indique le nombre de fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant. Le tableau 2 comporte une liste des N (où N est un nombre entier) premiers ordinateurs par quantités de données copiées. Il comporte les colonnes suivantes: • **Computer Name** Indique le nom de l'ordinateur • **Data Size** Indique la taille totale de tous les fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant.

TYPE DE RAPPORT	DESCRIPTION
Top active users	Ce rapport indique les utilisateurs les plus actifs, triés en fonction du nombre de fichiers copiés et de la taille totale de tous les fichiers copiés. Par défaut, il comporte une liste des 10 premiers utilisateurs mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. *Le format de date/heure des champs Period from: et to: est fonction du format de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise Server est exécuté*. • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Channel(s):** montre les types de périphériques et/ou les protocoles spécifiés pour le rapport. • **File Name:** Indique les fichiers concernés par le rapport en question. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) premiers utilisateurs par nombre de fichiers copiés. Il comporte les colonnes suivantes: • **User Name** Indique le nom de l'utilisateur • **Number of Files** Indique le nombre de fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant. Le tableau 2 comporte une liste des N (où N est un nombre entier) premiers utilisateurs par quantités de données copiées. Il comporte les colonnes suivantes: • **User Name** Indique le nom de l'utilisateur • **Data Size** Indique la taille totale de tous les fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant.
Top copied files	Ce rapport indique les fichiers les plus souvent copié, triés en fonction du nombre de fichiers copiés et de la taille totale de tous les fichiers copiés. Par défaut, il comporte une liste des 10 premiers fichiers mais vous pouvez modifier ce nombre en fonction de vos besoins. Il comporte trois sections: l'en-tête de rapport, les paramètres de rapport et les résultats de rapport. La section En-tête de rapport contient le titre de rapport qui apparaît en tout début de rapport. Le titre du rapport indique le type de rapport. La section Paramètres de rapport contient des informations sur les paramètres de rapport choisis lors de la création du rapport. Ces informations concernent notamment les paramètres: • **Period from: to:** Indiquent les dates de début et de fin de la période de rapport pour laquelle les données sont affichées. Le format de date/heure des champs Period from: et to: est fonction du format *de date/heure du compte d'utilisateur dans lequel DeviceLock Enterprise*

TYPE DE RAPPORT	DESCRIPTION
	Server est exécuté. • **Computer(s):** Indique les ordinateurs concernés par le rapport. • **Channel(s):** montre les types de périphériques et/ou les protocoles spécifiés pour le rapport. • **Users(s):** Indique les utilisateurs concernés par le rapport. La section Résultats de rapport contient deux tableaux avec les résultats détaillés du rapport. Le tableau 1 comporte une liste des N (où N est un nombre entier) fichiers les plus copiés par quantité. Il comporte les colonnes suivantes: • **File Name** Indique le nom de fichier • **Number of Files** Indique le nombre de fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant. Le tableau 2 comporte une liste des N (où N est un nombre entier) fichiers les plus copiés par taille. Il comporte les colonnes suivantes: • **File Name** Indique le nom de fichier • **Data Size** Indique la taille totale de tous les fichiers copiés. Les valeurs de cette colonne sont triées par ordre décroissant.

Configuration d'envoi de rapports par e-mails

DeviceLock permet de diffuser des rapports par e-mails. L'envoi de rapports par e-mails nécessite un serveur SMTP (Simple Mail Transport Protocol). Pour pouvoir utiliser l'envoi des rapports par e-mails, vous devez indiquer le serveur SMTP utilisé pour envoyer les e-mails et l'adresse de messagerie utilisée en tant qu'adresse d'émetteur.

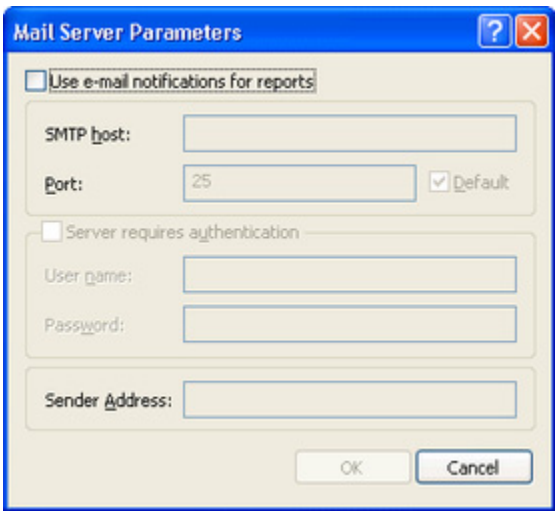
Pour configurer l'envoi des rapports par e-mails

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur qui exécute DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, cliquez droit sur **Reports**, puis cliquez sur **Notification Settings**.

   – OU -

   Sélectionnez **Reports**, puis cliquez sur l'option **Notification Settings** de la barre d'outils.

   La boîte de dialogue Mail Server Parameter s'ouvre.



4. Dans la boîte de dialogue **Mail Server Parameter**, effectuez les actions suivantes:

UTILISER CECI	POUR FAIRE CELA
Use e-mail notifications for reports	Configurer un e-mail de notification pour les rapports remplis. Cocher la case **Use e-mail notifications for reports** pour pouvoir saisir vos informations d'e-mail dans les champs correspondants. Décocher la case **Use e-mail notifications for reports** pour supprimer le serveur SMTP précédemment configuré et les paramètres de notification par e-mail.
SMTP host	Indiquer le nom du serveur SMTP à utiliser lors de l'envoi de messages. Vous pouvez indiquer le serveur SMTP via une adresse IP ou un nom de DNS identifiable.
Port	Indiquer le port utilisé par les clients SMTP pour se connecter au serveur SMTP. Par défaut, il s'agit du port 25.
Server requires authentication	Indiquer le type d'authentification à utiliser avec le serveur SMTP. Cocher la case **Server requires authentication** pour indiquer une authentification de base. Décocher la case **Server requires authentication** pour supprimer l'authentification.
User name	Indiquer le nom d'utilisateur à utiliser pour l'authentification avec le serveur SMTP. Cette propriété nécessite une valeur si vous avez sélectionné une authentification de base.
Password	Indiquer le mot de passe à utiliser pour l'authentification avec le serveur SMTP. Cette propriété nécessite une valeur si vous avez sélectionné une authentification de base.
Sender Address	Indiquer l'adresse de messagerie à utiliser dans le champ **From**: d'un

UTILISER CECI	POUR FAIRE CELA
	e-mail.

5. Cliquez sur **OK**.

Configuration de format de rapports par défaut

Vous pouvez indiquer le format de sortie à utiliser pour vos rapports. Les options disponibles sont les suivantes:

- Format HTML (*.htm)
- Format PDF (*.pdf)
- Format Rich Text (*.rtf)

Par défaut, DeviceLock utilise PDF comme format de sortie des rapports.

Pour configurer le format de rapports par défaut

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, cliquez droit sur **Reports**. Puis sélectionnez **Set Default Format** et cliquez sur l'une ou l'autre des options suivantes: **HTML**, **PDF** ou **RTF**.

Définition de paramètres de rapport

Les paramètres de rapport permettent de préciser les données des fichiers de journaux DeviceLock à utiliser dans un rapport. Par exemple, vous pouvez préciser une plage de dates pour restreindre les données qui apparaissent dans le rapport. Les paramètres de rapport doivent être définis pour chaque rapport de façon individuelle. Pour définir des paramètres de rapport, utilisez la boîte de dialogue **Report Options**. Cette boîte de dialogue apparaît dans une des situations suivantes:

- Lorsque vous cliquez droit sur un modèle de rapport dans l'arborescence de console, puis cliquez sur **New Report**.
- Lorsque vous sélectionnez un modèle de rapport dans l'arborescence de console, puis cliquez sur l'option **New report** de la barre d'outils.

Boîte de dialogue Report Options

Period from:……To:
Indique les dates et heures de début et de fin de la période de rapport pour laquelle les données sont affichées. Le format de date est *MM/JJ/AAAA* où *MM* indique le mois, *JJ* le

jour, *AAAA* l'année. Le format d'heure est *hh:mm:ss* {AP}M, où *hh* indique l'heure, *mm* les minutes, *ss* les secondes, et {AP}M le matin ou l'après-midi.

Dans les champs **Period from:** et **To:** saisissez ou sélectionnez la date et l'heure de la période de rapport.

Les heures de début et de fin par défaut du rapport délimitent la période d'ouverture de la boîte de dialogue **Report Options**. La date de fin par défaut de la période de rapport est la date actuelle. Par défaut, la période de rapport débute exactement un mois avant la date de fin. Par exemple, si la date actuelle est le 5 mars 2009, la date de fin par défaut de la période de rapport est le 3/5/2009 (5 mars 2009) et la date de début par défaut le 2/5/2009 (5 février 2009).

Computer(s):
Indique les ordinateurs concernés par le rapport. Le champ **Computer(s)** ne figure pas dans la boîte de dialogue **Report Options** des rapports de type Top active computers .

Par défaut, le champ **Computer(s)** est vide. Autrement dit, le rapport affiche les données de tous les ordinateurs de la base de données du DeviceLock Enterprise Server.

Pour sélectionner les ordinateurs concernés par le rapport, procédez comme suit (au choix):

- Dans le champ **Computer(s)**, saisissez les noms des ordinateurs à l'aide de jokers comme les astérisques (*) et les points d'interrogation (?). Par exemple, si vous indiquez ***.mydomain.com**, le rapport affichera les données de tous les ordinateurs de mydomain.com.

  Un astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser un nombre quelconque de ces jokers à n'importe quel endroit.

  Les noms d'ordinateurs doivent être séparés par une virgule (,) ou un point-virgule (;).

  – OU -

- Cliquez sur le bouton **Browse** situé en regard du ou des **Computer(s):**, puis (au choix):

  a) Lorsque la boîte de dialogue **Edit computers list** s'ouvre pour afficher la liste **Select computer(s)**, cliquez sur une des options suivantes:

OPTION	DESCRIPTION
From Database	Cette option est sélectionnée par défaut. Cette option permet de sélectionner les ordinateurs dans la base de données de DeviceLock Enterprise Server. Cette base de données contient tous les ordinateurs ayant déjà envoyé des données d'audit et de réplication au serveur. Si vous sélectionnez cette option, 1. Dans le panneau de gauche de la boîte de dialogue, cochez les cases situées en regard des ordinateurs appropriés.

OPTION	DESCRIPTION
	2. Cliquez sur le bouton comportant une flèche simple vers la droite . *Les ordinateurs sélectionnés figurent dans le champ Selected computers du panneau droit de la boîte de dialogue.* *Pour supprimer un à un des ordinateurs de la liste des ordinateurs sélectionnés, utilisez le bouton comportant une flèche simple vers la gauche* . *Pour ajouter ou supprimer en même temps tous les ordinateurs disponibles d'une liste d'ordinateurs sélectionnés, utilisez le bouton comportant une double flèche vers la droite* *ou le bouton comportant une double flèche vers la gauche* .
From File	Cette option permet de sélectionner des ordinateurs dans un fichier de texte externe. Un fichier de texte doit impérativement comporter le nom de chaque ordinateur ou son adresse IP sur des lignes séparées et peut être indifféremment en format Unicode ou non-Unicode. Si vous sélectionnez cette option, 1. Cliquez sur le bouton comportant des points de suspension pour ouvrir la boîte de dialogue **Open** et naviguer vers le fichier à utiliser. 2. Dans la boîte de dialogue **Open** de la liste de Look in, cliquez sur l'emplacement contenant le fichier que vous souhaitez importer. 3. Dans la liste des dossiers, localisez et ouvrez le dossier qui contient le fichier. 4. Cliquez sur le fichier puis sur **Open**. *Les ordinateurs du fichier figurent dans le panneau gauche de la boîte de dialogue Modifier la liste des ordinateurs*. 5. Dans le panneau gauche de la boîte de dialogue **Edit computers**, sélectionnez les ordinateurs souhaités, puis cliquez droit sur le bouton comportant une flèche simple vers la droite . *Les ordinateurs sélectionnés figurent dans le champ Selected computers du panneau droit de la boîte de dialogue.* *Pour supprimer un à un des ordinateurs de la liste des ordinateurs sélectionnés, utilisez le bouton comportant une flèche simple vers la gauche* . *Pour ajouter ou supprimer en même temps tous les ordinateurs disponibles d'une liste d'ordinateurs sélectionnés, utilisez le bouton comportant une double flèche vers la droite* *ou le bouton comportant une double flèche vers la gauche* .
Manual	Cette option permet d'ajouter manuellement les ordinateurs que vous souhaitez sélectionner pour le rapport. Si vous sélectionnez cette option, 1. Dans le panneau gauche de la boîte de dialogue **Edit computers list**, saisissez soit les noms des ordinateurs, soit leurs adresses IP. Appuyez sur la touche ENTER après chaque nom d'ordinateur afin que chacun d'entre eux figure sur une ligne séparée. 2. Dans le panneau gauche de la boîte de dialogue **Edit computers**, sélectionnez les ordinateurs souhaités, puis cliquez droit sur le bouton comportant une flèche simple vers la droite . *Les ordinateurs sélectionnés figurent dans le champ Selected*

OPTION	DESCRIPTION
	computers du panneau droit de la boîte de dialogue. *Pour supprimer un à un des ordinateurs de la liste des ordinateurs sélectionnés, utilisez le bouton comportant une flèche simple vers la gauche* . *Pour ajouter ou supprimer en même temps tous les ordinateurs disponibles d'une liste d'ordinateurs sélectionnés, utilisez le bouton comportant une double flèche vers la droite* *ou le bouton comportant une double flèche vers la gauche* .

b) Cliquez sur **OK**.

Users
Indique les utilisateurs concernés par le rapport. Le champ **User(s)** ne figure pas dans la boîte de dialogue **Report Options** des rapports de type Top active computers et Top active users.

Par défaut, le champ **User(s)** est vide. Autrement dit, le rapport affiche les données de tous les utilisateurs de la base de données du DeviceLock Enterprise Server.

Pour indiquer les utilisateurs concernés par le rapport, procédez comme suit (au choix):

- Dans le champ **User(s)**, saisissez les noms des utilisateurs à l'aide de jokers comme les astérisques (*) et les points d'interrogation (?). Par exemple, si vous indiquez **mydomain***, le rapport affichera les données de tous les ordinateurs de mydomain.com.
  Un astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser un nombre quelconque de ces jokers à n'importe quel endroit.

  Les noms d'utilisateurs doivent être séparés par une virgule (,) ou un point-virgule (;).

  Remarque: Vous ne pouvez pas indiquer des groupes d'utilisateurs pour le rapport.

  – OU -

- Cliquez sur le bouton **Browse** situé en regard du champ **User(s)**, puis procédez comme suit (au choix):
  a) Dans la boîte de dialogue **Select Users** qui s'ouvre, saisissez les noms des comptes d'utilisateurs que vous souhaitez indiquer pour le rapport dans le champ **Enter the object names to select**.
  Les noms d'utilisateurs doivent être séparés par un point-virgule (;).
  b) Cliquez sur **OK**.

Threshold
Indique l'intervalle de temps, en secondes, entre événements de journal. Cet intervalle sert à consolider les événements. Il figure dans tous les types de rapports de la catégorie Audit Log report, hormis les rapports de type Top inserted USB & FireWire devices.

Comme une action utilisateur individuelle déclenche souvent plusieurs événements, DeviceLock utilise la consolidation d'événements pour recueillir les événements du journal d'audit servant au reporting. DeviceLock compare la durée d'un événement à celle des événements suivants. Lorsque cet écart de temps est inférieur ou égal à la valeur de **Threshold**, plusieurs éléments du même type (soit Autorisé, soit Refusé) sont associés en un événement de résumé unique si toutes les conditions suivantes sont réunies:

- Les événements sont associés au même ordinateur
- Les événements sont associés au même type de périphérique

Report Devices
Sélectionner cette option pour afficher les données pour tous les types de périphériques. Si vous ne sélectionnez pas cette option, les informations sur les activités liées aux périphériques seront exclues de ce rapport. Ne s'affiche que pour les types de rapports suivants: les demandes d'accès autorisées et refusées par canal, les demandes d'accès autorisées et refusées, et les fichiers copiés par canal.

Report Protocols
Sélectionner cette option pour afficher les données pour tous les protocoles. Si vous ne sélectionnez pas cette option, les informations sur les activités liées aux protocoles seront exclues de ce rapport. Ne s'affiche que pour les types de rapports suivants: les demandes d'accès autorisées et refusées par canal, les demandes d'accès autorisées et refusées, et les fichiers copiés par canal.

Send report via email
Sélectionnez cette option pour envoyer automatiquement par e-mail le rapport généré à des utilisateurs individuels. Si vous sélectionnez cette option, saisissez les adresses de messagerie des destinataires dans le champ **Recipients**, séparées par des virgules, des points-virgules ou des espaces. Utilisez le format suivant: *user*@*mailserver*

Access type(s)
Indique les types d'événements que vous souhaitez inclure ou exclure du rapport. N'apparaît que pour les rapports de type Read & Write access requests per device type dans la catégorie Audit Log report.

Si vous cochez la case **Allowed**, le rapport contiendra les événements Success Audit (autrement dit, ceux faisant état de tentatives d'accès réussies). Si vous cochez la case **Denied**, le rapport contiendra les événements Failure Audit (autrement dit, ceux faisant état de tentatives d'accès refusées). Vous pouvez utiliser soit l'une, soit l'autre, soit les deux options pour indiquer les types d'événements.

Device type(s)
Indique les types de périphériques concernés par le rapport. Ne s'affiche que pour les rapports de types Top active computers, Top active users, et Top copied files.

Si vous utilisez cette option, cochez les cases appropriées en regard des types de périphériques que vous souhaitez inclure dans le rapport.

Protocol(s)
Spécifie les protocoles pour le rapport. Ne s'affiche que pour les types de rapports suivants : ordinateurs les plus actifs, utilisateurs les plus actifs et fichiers les plus copiés.

Si vous sélectionnez cette option, cochez les cases appropriées en regard des protocoles que vous souhaitez spécifier pour le rapport.

Remarque: Si vous omettez de sélectionner les deux options: **Device type(s)** et **Protocol(s)**, le rapport affichera les données pour tous les types de périphériques et les protocoles. Si vous sélectionnez l'une ou l'autre de ces options, puis indiquez des types de périphériques ou des protocoles, le rapport n'affichera des données que pour les types de périphériques ou les protocoles spécifiés.

Top computers
Indique le nombre des ordinateurs les plus fréquemment utilisés. Ne s'affiche que pour les rapports de type Top active computers.

Par défaut, la valeur est 10. Pour la changer, saisir ou sélectionner le nombre d'ordinateurs appropriés dans le champ **Top computers**.

Top users
Indique le nombre des utilisateurs les plus actifs. Ne s'affiche que pour les rapports de type Top active users.

Par défaut, la valeur est 10. Pour la changer, saisir ou sélectionner le nombre d'utilisateurs appropriés dans le champ **Top users**.

Top USB and FireWire devices
Indique le nombre des périphériques USB et FireWire les plus fréquemment utilisés. Ne s'affiche que pour les rapports de type Top inserted USB & FireWire devices.

Par défaut, la valeur est 10. Pour la changer, saisir ou sélectionner le nombre de périphériques appropriés dans le champ **Top USB and FireWire devices**.

Top USB devices
Indique le nombre des périphériques USB les plus fréquemment utilisés. Ne s'affiche que pour les rapports de type Top used USB devices.

Par défaut, la valeur est 10. Pour la changer, saisir ou sélectionner le nombre de périphériques appropriés dans le champ **Top USB devices**.

File name
Indique les fichiers concernés par le rapport. N'apparaît que pour les rapports de type Top active users, Top active computers et Copied files per channel dans la catégorie Shadow Log report.

Par défaut, le champ **File name** est vide. Autrement dit, le rapport affiche les données de tous les fichiers de la base de données du DeviceLock Enterprise Server.

Pour indiquer les fichiers concernés par le rapport, saisissez les noms de fichiers dans le champ **File name** à l'aide de joker comme les astérisques (*) et les points d'interrogation (?). Par exemple, saisissez ***.txt** pour indiquer tous les fichiers comportant l'extension .txt. De même, pour sélectionner tous les fichiers dont les noms commencent par une suite de caractères contenant la séquence «prix» et d'extension quelconque, saisissez ***price*.***

Un astérisque (*) remplace un nombre illimité de caractères. Le point d'interrogation (?) remplace un caractère simple. Vous pouvez utiliser un nombre quelconque de ces jokers à n'importe quel endroit.

Les noms de fichiers doivent être séparés par une virgule (,) ou un point-virgule (;).

Gestion de rapports

La gestion des rapports DeviceLock comporte les tâches suivantes:

- Exécution de rapports
- Mise à jour de rapports
- Affichage de rapports
- Affichage de paramètres de rapports
- Exportation et enregistrement de rapports
- Envoi de rapports par e-mail
- Suppression de rapports

Exécution de rapports

Pour exécuter un rapport

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, cliquez droit sur le modèle de rapport que vous souhaitez utiliser, puis cliquez sur **New report**.

   La boîte de dialogue Report Options apparaît.
6. Dans la boîte de dialogue **Report Options**, acceptez ou changez les paramètres par défaut, puis cliquez sur **OK**.

   Pour en savoir plus sur les paramètres par défaut et leur modification dans la boîte de dialogue Report Options, consultez la section «Définition de paramètres de rapport.»

   Pendant que le rapport est traité sur DeviceLock Enterprise Server, les informations d'exécution de rapport sont affichées dans DeviceLock Management Console. Pour afficher et analyser ces informations, sélectionnez dans l'arborescence de console le modèle de rapport que vous avez utilisé pour exécuter un nouveau rapport.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence de console, le panneau de détails affiche les informations d'exécution de rapport concernant tous les rapports basés sur le modèle sélectionné. Les informations d'exécution de rapport incluent les éléments suivants:

   - **User** Le nom de l'utilisateur qui a exécuté le rapport.
   - **From Computer** Le nom de l'ordinateur utilisé pour exécuter le rapport.
   - **Started** La date et l'heure de début d'exécution du rapport.
   - **Finished** La date et l'heure de fin d'exécution du rapport.
   - **E-mailed** Valeurs possibles: **Yes** et **No**. **Yes** indique que le rapport inclus dans le courriel a bien été remis à certains des destinataires envisagés ou à l'ensemble d'entre eux. **Yes** ne s'affiche qu'une fois le processus d'envoi terminé. **No** indique un des événements suivants:

     Le rapport n'est pas inclus dan le courriel.

     – OU -

     Le rapport inclus dans le courriel n'est pas parvenu à l'ensemble des destinataires envisagés.

     En cas d'erreur lors de l'envoi d'un rapport par e-mail, vous pouvez utiliser le Server Log Viewer pour en déterminer le motif. Pour en savoir plus sur le Server Log Viewer, voir «Server Log Viewer.»

     Si votre ordinateur comporte un logiciel antivirus ou anti-spam installé et actif, et si une erreur s'est produite lors de l'envoi par e-mail d'un rapport, il se peut que l'erreur ne figure pas dans le journal du DeviceLock Enterprise Server. Ceci parce que les antivirus et les anti-spams, l'antivirus Symantec Norton par exemple, peuvent intercepter automatiquement le trafic de messagerie.

Pour en savoir plus sur la façon dont votre logiciel antivirus ou anti-spam fonctionne, consultez la documentation du fabricant incluse dans votre logiciel.

- **Status** Valeurs possibles: **Generating**, **Ready**, **Error**. **Generating** indique que le rapport est en cours de génération. **Ready** indique que le rapport a bien été généré. **Error** indique qu'une erreur s'est produite en cours de génération du rapport.

  Si une erreur se produit pendant la génération du rapport, vous pouvez en déterminer l'origine en:

  Cliquant sur le rapport d'erreur pour afficher le message d'erreur.

  – OU -

  En utilisant le Server Log Viewer. Pour en savoir plus sur le Server Log Viewer, voir «Server Log Viewer.»

Mise à jour de rapports

Etant donné que ni les rapports actuels ni leurs statuts ne sont mis à jour automatiquement, il faut effectuer manuellement cette mise à jour.

Pour mettre à jour des rapports

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, cliquez droit sur n'importe quel modèle de rapport, puis cliquez sur **Refresh**.

   – OU -

   Dans **Audit Log** ou **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour les rapports de génération, puis procédez comme suit (au choix):

   - Cliquez sur l'option **Refresh** de la barre d'outils.

     – OU -
   - Dans le panneau de détails, cliquez droit sur n'importe quel rapport, puis cliquez sur **Refresh**.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

Affichage de rapports

Une fois un rapport élaboré, vous pouvez l'ouvrir dans la DeviceLock Management Console.

Pour afficher un rapport

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.

3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour générer le rapport que vous souhaitez consulter.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

6. Dans le panneau de détails, cliquez droit sur le rapport que vous souhaitez consulter, puis cliquez sur **Open**.

   Le rapport s'ouvre dans l'application associée avec le format de rapport par défaut que vous avez choisi. Par défaut, le rapport s'ouvre dans Adobe Acrobat Reader, car DeviceLock utilise PDF en tant que format de sortie par défaut pour les rapports.

   Pour ouvrir un rapport au format PDF, votre ordinateur doit être doté d'Adobe Acrobat Reader. Vous pouvez télécharger Acrobat Reader sur le site web d'Adobe: http://get.adobe.com/reader/.

Affichage de paramètres de rapports

Une fois le rapport exécuté, vous pouvez obtenir des informations sur les paramètres de rapport que vous avez précisés lors de la génération du rapport.

Pour afficher des paramètres de rapport

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour générer le rapport.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

6. Dans le panneau de détails, cliquez droit sur le rapport, puis cliquez sur **View parameters**.

   La boîte de dialogue Report Options apparaît. Dans cette boîte de dialogue, vous pouvez consulter les valeurs des paramètres que vous avez spécifiées lors de la génération du rapport.

Exportation et enregistrement de rapports

DeviceLock permet d'exporter les rapports générés dans un autre format (comme HTML, PDF ou RTF) et de les enregistrer sous forme de fichiers locaux ou sur votre réseau.

Remarque: Lorsque vous enregistrez un rapport au format HTML, il est enregistré sous forme de fichier .html. Si ce rapport contient des images graphiques, chaque image est enregistrée sous forme de fichier .gif dans le même répertoire que le fichier .htm.

Pour exporter et enregistrer des rapports

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour générer le rapport que vous souhaitez exporter et enregistrer.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

6. Pour exporter et enregistrer un rapport individuel, procédez comme suit:
   a) Dans le panneau de détails, cliquez droit sur le rapport que vous souhaitez exporter et enregistrer, pointez sur **Save As**, puis cliquez sur l'une ou l'autre des options suivantes: **HTML**, **PDF** ou **RTF**.
      La boîte de dialogue Save as apparaît.
   b) Dans la boîte de dialogue **Save As**, naviguez vers l'emplacement où vous souhaitez enregistrer le rapport.
   c) Dans le champ de nom **File**, saisissez le nom de fichier souhaité.
      Par défaut, le nom de fichier est {Type de rapport}- [{jj.mm.aa hh:mm:ss}] où {jj.mm.aa hh:mm:ss} sont la date et l'heure actuelle.
   d) Cliquez sur **Save**.

      Si vous enregistrez un rapport au format HTML et qu'il contient une ou plusieurs images graphiques, celles-ci seront extraites du rapport et enregistrées sous forme de fichiers .gif séparés en plus du fichier .htm dans le même répertoire.

   Pour exporter et enregistrer plusieurs rapports, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs rapports en maintenant enfoncée la touche MAJ ou la touche CTRL tout en cliquant sur les rapports en question.
   b) Cliquez droit sur la sélection, pointez sur **Save As**, puis cliquez sur l'une ou l'autre des options suivantes: **HTML**, **PDF** ou **RTF**.
      La boîte de dialogue Browse for folder apparaît.
   c) Dans la boîte de dialogue **Browse for folder**, sélectionnez le dossier dans lequel vous souhaitez enregistrer les rapports, puis cliquez sur **OK**.

Envoi de rapports par e-mail

DeviceLock permet d'envoyer les rapports générés par e-mail.

Pour envoyer des rapports générés par e-mail

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** or **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour générer le rapport que vous souhaitez envoyer par e-mail.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

6. Dans le panneau de détails, cliquez droit sur le rapport que vous souhaitez envoyer, puis cliquez sur **Send via e-mail**.

   Vous pouvez sélectionner plusieurs rapports en maintenant enfoncée la touche MAJ ou la touche CTRL tout en cliquant sur les rapports en question.

   La boîte de dialogue Send report via e-mail apparaît.

7. Dans la boîte de dialogue **Send report via e-mail**, dans la boîte **Recipients**, saisissez les adresses de messagerie des destinataires séparés par des virgules, des points-virgules ou des espaces. Utilisez le format suivant : *user@mailserver.*
8. Cliquez sur **OK**.

   Si une erreur se produit lors de l'envoi d'un rapport par e-mail, le message d'erreur correspondant est consigné dans le journal. Vous pouvez utiliser le Server Log Viewer pour en déterminer le motif. Pour en savoir plus sur le Server Log Viewer, voir «Server Log Viewer.»

Remarque: Lorsque vous envoyez un rapport au format HTML, celui-ci figure dans le corps de l'e-mail et non en tant que pièce jointe.

Suppression de rapports

Vous pouvez supprimer des rapports lorsqu'ils ne sont plus nécessaires.

Pour supprimer des rapports

1. Ouvrez la DeviceLock Management Console et connectez-la à l'ordinateur exécutant DeviceLock Enterprise Server.
2. Dans l'arborescence de console, développez **DeviceLock Enterprise Server**.
3. Dans **DeviceLock Enterprise Server**, développez **Reports**.
4. Développez **Audit Log** ou **Shadow Log**.
5. Dans **Audit Log** ou **Shadow Log**, sélectionnez le modèle de rapport que vous avez utilisé pour générer le rapport que vous souhaitez supprimer.

   Lorsque vous sélectionnez un modèle de rapport dans l'arborescence, vous pouvez afficher les rapports associés dans le panneau de détails.

6. Dans le panneau de détails, cliquez droit sur le rapport que vous souhaitez supprimer, puis cliquez sur **Delete**.

Vous pouvez supprimer plusieurs rapports en même temps. Pour ce faire, procédez comme suit :

a) Dans le panneau de détails, sélectionnez plusieurs rapports en maintenant enfoncée la touche MAJ ou la touche CTRL tout en cliquant sur les rapports en question.
b) Cliquez droit sur la sélection, puis cliquez sur **Delete**.

Politiques de sécurité de DeviceLock (Offline Profile)

Aujourd'hui, nombreux sont les utilisateurs qui doivent pouvoir continuer à travailler avec des informations commerciales stratégiques même lorsqu'ils ne sont plus connectés au réseau de leur organisation. Ainsi, les représentants de commerce itinérants, les agents d'assurance et les inspecteurs régionaux utilisent laptops et notebooks d'entreprise en dehors des sites connectés. La protection des informations sensibles sur ces ordinateurs portables est devenue une priorité pour de nombreuses organisations.

DeviceLock permet une meilleure protection des informations d'entreprise sensibles dans les environnements non connectés. Vous pouvez désormais contrôler l'accès des utilisateurs aux périphériques et aux protocoles, ainsi que la réplication des données écrites par l'utilisateur ou transmises sur le réseau dans différents scénarios hors ligne. DeviceLock permet aussi une plus grande flexibilité de gestion, car vous pouvez définir différentes politiques de sécurité en ligne ou hors ligne pour le même utilisateur ou ensemble d'utilisateurs.

Les politiques d'utilisation en ligne sont appliquées en cas de connexion au réseau d'entreprise, aux DeviceLock Enterprise Servers indiqués, ou aux contrôleurs de domaine Active Directory. Les politiques hors ligne sont appliquées en cas de travail hors connexion avec le réseau d'entreprise, les DeviceLock Enterprise Servers indiqués, ou les contrôleurs de domaine Active Directory.

Pour configurer DeviceLock et appliquer différentes politiques de travail en ligne et hors ligne, commencez par définir les autorisations pour deux types de profils:

- **Regular Profile** (profil habituel). Ces paramètres sont utilisés par les ordinateurs client qui travaillent en ligne.
- **Offline Profile** (profil hors ligne). Ces paramètres sont utilisés par les ordinateurs client qui travaillent hors ligne, par exemple lorsque des utilisateurs d'entreprise voyagent avec des ordinateurs portables. Si les paramètres de profil hors ligne ne sont pas configurés, les paramètres de profil habituels sont utilisés à leur place.

Vous pouvez utiliser différents profils habituels ou hors ligne pour les paramètres Permissions (autorisations), Auditing and Shadowing (audit et réplication), USB Devices White List (liste blanche de périphériques USB), Media White List (liste blanche des média), Protocols White List (liste blanche de protocoles), Content-Aware Rules (règles contextuelles), et Security Settings (paramètres de sécurité). Vous pouvez gérer hors ligne les paramètres de profil à l'aide de la DeviceLock Management Console, du DeviceLock Service Settings Editor ou du DeviceLock Group Policy Manager.

Les exemples suivants décrivent des scénarios types dans lesquels vous pouvez être amené à définir différentes politiques de sécurité en et hors ligne pour mieux protéger vos données d'entreprise.

- **Scénario 1.** Supposez que vous disposiez d'un groupe Finance dans votre organisation. En tant qu'administrateur, vous pouvez autoriser les membres de ce groupe à inscrire des fichiers sur des périphériques de type Removable (amovible), DVD/CD-ROM, USB et Floppy lorsqu'ils fonctionnent en ligne. Leur activité en ligne fera l'objet d'un audit. Tout fichier copié le sera en mode de réplication, et les journaux d'audit et de réplication seront envoyés au DeviceLock Enterprise Server. Une fois hors ligne, les membres du groupe Finance n'auront plus le droit d'accéder en écriture au système.

  Ces politiques de sécurité permettent de surveiller l'activité des membres du groupe Finance en temps réel. En examinant les journaux d'audit et de réplication du DeviceLock Enterprise Server (souvent de façon quotidienne), vous pouvez réagir de façon rapide et appropriée en cas de fuite de données. Dans ce cas, un utilisateur ne pourra pas copier des informations sensibles sur un périphérique lorsqu'il est hors ligne de peur d'envoyer des copies de réplication au DeviceLock Enterprise Server et d'alerter par là-même le département Sécurité des données volées.

- **Scénario 2.** Imaginez Marie, agent commercial d'une grande société, qui dispose d'un notebook et travaille fréquemment hors de son bureau. Elle doit pouvoir fournir à ses partenaires commerciaux des fichiers d'informations liés à son travail. Dans ce cas, vous pouvez autoriser Marie à inscrire certains fichier sur des périphériques de type amovible, DVD/CD-ROM, USB et Floppy, et lui permettre la copie de réplication de ces fichiers lorsqu'elle travaille hors ligne. Une fois en ligne, elle n'aura plus accès en écriture aux types de périphériques en question.

  Ces politiques de sécurité rendent plus flexible la gestion des utilisateurs au sein d'une organisation, tout en permettant d'augmenter la sécurité des données de l'entreprise.

Configuration de paramètres de détection de mode hors ligne

Vous pouvez définir les caractéristiques du réseau que DeviceLock utilise pour détecter son statut de connexion (s'il est en ou hors ligne). Par défaut, DeviceLock fonctionne en mode hors ligne lorsque le câble réseau n'est pas connecté à l'ordinateur client.

Pour configurer les paramètres de détection de mode hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

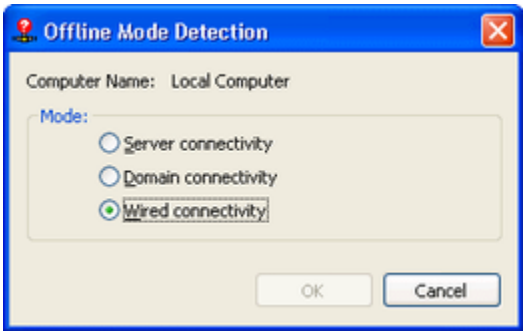
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Sélectionnez **Service Options**.

   Lorsque vous sélectionnez les Service Options dans l'arborescence, celles-ci s'affichent dans le panneau de détails.

3. Dans le panneau de détails, procédez comme suit (au choix):
   - Cliquez droit sur **Offline mode detection**, puis sur **Properties**.
     - OU -
   - Double-cliquez sur **Offline mode detection**.

   La boîte de dialogue Offline Mode Detection apparaît.



4. Dans la boîte de dialogue **Offline Mode Detection**, cliquez sur l'une ou l'autre des options suivantes:

OPTION	DESCRIPTION
Server connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de sa capacité (ou non) à se connecter au DeviceLock Enterprise Server indiqué. Autrement dit, un ordinateur client fonctionne en mode en ligne s'il peut se connecter à l'un ou l'autre des DeviceLock Enterprise Server indiqués et leur envoyer des journaux d'audit et de réplication. Un ordinateur client fonctionne en mode hors ligne s'il ne peut s'identifier auprès des DeviceLock Enterprise Server indiqués ou si tous les DeviceLock Enterprise Server indiqués sont indisponibles en même temps. **Pratiques éprouvées:** La meilleure façon pour fiabiliser la communication client/serveur est d'utiliser l'authentification par DeviceLock Certificate. Pour l'authentification des certificats client/serveur, la clé publique doit être installée sur les ordinateurs client, alors que la clé privée doit être installée sur les DeviceLock Enterprise Server. Si le certificat (la clé privée) n'est installé que sur le DeviceLock Enterprise Server, le serveur refusera les connexions et les ordinateurs client fonctionneront en mode hors ligne. Si le certificat (la clé publique) n'est installé que sur les ordinateurs client, le serveur et le client s'identifieront l'un l'autre une fois la connexion établie, même si ce type d'authentification est moins sûr que l'authentification à base de certificats. Pour en savoir plus sur les DeviceLock Certificates, consultez le chapitre

OPTION	DESCRIPTION
	«DeviceLock Certificates.»
Domain connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de sa capacité (ou non) à se connecter au contrôleur de domaine Active Directory approprié (à un contrôleur de domaine du domaine auquel l'ordinateur client appartient). Dans ce cas de figure, un ordinateur client fonctionne en mode en ligne s'il peut se connecter au contrôleur de domaine approprié. Un ordinateur client fonctionne en mode hors ligne dès lors que le contrôleur de domaine approprié n'est plus disponible. *Un ordinateur client non relié à un domaine (un groupe de travail ou un ordinateur autonome) fonctionne toujours en mode hors ligne.*
Wired connectivity	Indique que le statut de connexion d'un ordinateur client est fonction de la connexion (ou non) du câble de réseau au NIC (pour Network Interface Card, ou carte d'interface réseau). Il s'agit de la méthode la plus simple et la moins sure pour détecter le statut de connexion. Dans ce cas de figure, un ordinateur client fonctionne en mode en ligne si le câble de réseau est connecté au NIC. Un ordinateur client fonctionne en mode hors ligne si le câble de réseau est déconnecté du NIC. Remarque : les connexions à des réseaux sans fils (Wi-Fi, etc.) et les connexions modem sont ignorées. Cette option est sélectionnée par défaut.

5. Cliquez sur **OK**.

Passage du mode en ligne au mode hors ligne

Lorsqu'il fonctionne sur des ordinateurs client, DeviceLock Service détecte automatiquement le statut de connexion et passe de façon transparente du mode en ligne au mode hors ligne toutes les heures et lorsque l'un ou l'autre des événements suivants se produit :

- Un utilisateur démarre l'ordinateur qui exécute DeviceLock Service.
  DeviceLock Service démarre toujours en mode hors ligne.

- Un utilisateur se connecte.
- Un utilisateur clique droit sur l'icône de DeviceLock Tray Notification Utility situé dans la zone de notification de la barre des tâches, puis clique sur **Refresh Current State**.
  L'icône DeviceLock Tray Notification Utility s'affiche dans la zone de notification lorsque l'option Always show tray icon (toujours afficher l'icône de barre) est activée dans les Service Options.

- DeviceLock Service envoie les journaux d'audit et de réplication à DeviceLock Enterprise Server.
- Une interface de réseau change de statut lorsque:
  - Un câble réseau est connecté ou déconnecté.

  - Un modem se connecte ou se déconnecte.
  - Une connexion VPN (pour virtual private network, ou réseau privé virtuel) est établie ou prend fin.
  - Une connexion réseau sans fil utilisant une carte Wi-Fi est établie ou prend fin.
  - Une adresse IP assignée par DHCP est utilisée ou libérée.
  - Une carte réseau est activée, désactivée, ajoutée ou supprimée.
- Des changements aux paramètres de DeviceLock Service sont effectués.

Gestion des politiques de sécurité hors ligne pour les périphériques

Vous pouvez gérer les politiques de sécurité hors ligne de façon très similaire à celle dont vous gérer les politiques en ligne (habituelles), hormis quelques variations. Cette section fournit des informations spécifiques aux profils hors ligne, ainsi que des procédures de gestion de base. Pour des informations détaillées sur les autorisations, les règles d'audit et de réplication, les listes blanches, les règles contextuelles et les paramètres de sécurité, reportez-vous aux sections suivantes du manuel d'utilisateur: «Autorisations (Regular Profile),» «Audit et réplication (Regular Profile),» «Liste blanche de périphériques USB (Regular Profile),» «Liste blanche de médias (Regular Profile),» «Paramètres de sécurité (Regular Profile),» «Règles contextuelles pour les périphériques (Regular Profile).»

La gestion des politiques de sécurité hors ligne pour les périphériques comprend les opérations suivantes:

- Gestion des autorisations hors ligne
- Gestion des règles d’audit et de réplication hors ligne
- Gestion de la liste blanche de périphériques USB hors ligne
- Gestion de la liste blanche de médias hors ligne
- Gestion des règles contextuelles hors ligne
- Gestion des paramètres de sécurité hors ligne

Vous pouvez gérer les politiques de sécurité hors ligne à l’aide des utilitaires DeviceLock Management Console, DeviceLock Service Settings Editor ou DeviceLock Group Policy Manager.

Gestion des autorisations hors ligne

Pour une descriptions détaillée de la fonction Autorisations, consultez le chapitre «Autorisations (Regular Profile).»

Les autorisations hors ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les autorisations ne sont pas définies pour le type de périphériques en question. Il s'agit du statut par défaut.
Configured	Indique que les autorisations sont définies pour le type de périphériques en question.
Full Access	Indique que le compte Everyone (tout le monde) bénéficie de tous les droits d'accès.
No Access	Indique une des situations suivantes: • Le compte Everyone (tout le monde) bénéficie d'autorisations No Access (pas d'accès) et est le seul compte assigné à un type de périphériques. *Les autorisations No Access (pas d'accès) assignées au compte Everyone (tout le monde) l'emportent sur les autorisations assignées aux autres comptes.* • Tous les utilisateurs et les groupes assignés à un type de périphériques bénéficient d'autorisations No Access (pas d'accès). • Tous les utilisateurs et les groupes assignés à un type de périphériques sont supprimés.
Use Regular	Indique que l'héritage des autorisations hors ligne est bloqué et que les autorisations habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des autorisations habituelles est utile si vous utilisez les fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des autorisations habituelles permet d'empêcher l'application des autorisations hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des autorisations habituelles, consultez le chapitre intitulé «Suppression d'autorisations hors ligne.»

La gestion des autorisations hors ligne comprend les tâches suivantes:

- Définition et édition d'autorisations hors ligne
- Révocation d'autorisations hors ligne
- Suppression d'autorisations hors ligne

Définition et édition d'autorisations hors ligne

Pour définir et éditer des autorisations hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.

b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

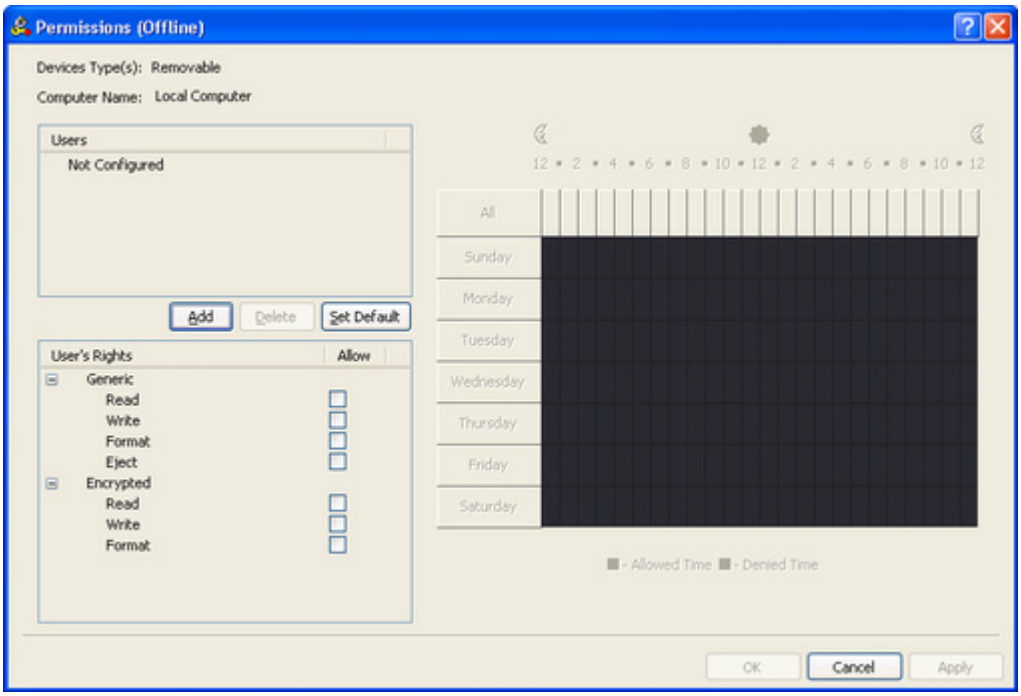
a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque type de périphériques dans la colonne Offline (hors ligne)

4. Dans le panneau de détails, procédez comme suit (au choix):
   - Cliquez droit sur le type de périphériques pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur **Set Offline Permissions**.
     - OU -
   - Sélectionnez le type de périphériques pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur le bouton **Set Offline Permissions** de la barre d'outils.

   La boîte de dialogue Permission (Offline) apparaît.



5. Dans la boîte de dialogue **Permissions (Offline)**, procédez comme suit:

POUR FAIRE CECI	PROCEDEZ COMME SUIT
Définir des	• Dans le champ Users du panneau supérieur gauche de la boîte

POUR FAIRE CECI	PROCEDEZ COMME SUIT
autorisations par défaut	de dialogue, cliquez sur **Set Default**. *Les autorisations par défaut sont assignées aux comptes Administrators, Everyone et SYSTEM. Pour en savoir plus sur les autorisations définies pour ces comptes par défaut, consultez le chapitre intitulé* «Autorisations (Regular Profile).»
Définir des autorisations pour un utilisateur ou un groupe supplémentaire	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît*. 2. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes ajoutés figurent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Permissions (Offline)*. 3. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue **Permissions (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs et/ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.* 4. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Permissions (Offline)**, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés. *Le panneau de droite de la boîte de dialogue Permissions (Offline) permet de définir les limites d'accès des utilisateurs aux périphériques en termes de jours et d'heures. Utilisez le bouton gauche de la souris pour sélectionner les jours et les horaires auxquels l'utilisateur ou le groupe sélectionné aura accès aux périphériques. Utilisez le bouton droit de la souris pour indiquer les jours et les horaires auxquels l'utilisateur ou le groupe sélectionné n'aura pas accès aux périphériques*.
Changer les autorisations d'un utilisateur ou d'un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés
Supprimer un utilisateur ou un groupe existant et ses autorisations	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation d'autorisations hors ligne

Vous pouvez redonner aux autorisations hors ligne précédemment définies le statut non configuré. Si les autorisations hors ligne sont non définies, les autorisations habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des autorisations hors lignes

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque type de périphériques dans la colonne Offline (hors ligne).
4. Dans le panneau de détails, cliquez droit sur le type de périphériques pour lequel vous souhaitez révoquer les autorisation hors ligne, puis cliquez sur **Undefine Offline**.

   Vous pouvez révoquer les autorisations offline définies pour plusieurs types de périphériques à la fois. Pour ce faire, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs types de périphériques et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine Offline**.

   Les autorisations adoptent alors le statut hors ligne «Not Configured» (non configuré).

Suppression d'autorisations hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage des autorisations hors ligne de niveau supérieur et d'appliquer les autorisations habituelles à certains groupes d'ordinateurs client de niveau inférieur. Pour que les autorisations habituelles s'appliquent, vous devez supprimer les autorisations hors ligne.

Pour supprimer des autorisations hors lignes

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

a) Ouvrez DeviceLock Service Settings Editor.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque type de périphériques dans la colonne Offline (hors ligne)

4. Dans le panneau de détails, cliquez droit sur le type de périphériques pour lequel vous souhaitez supprimer les autorisations hors ligne, puis cliquez sur **Remove Offline**.

   Vous pouvez supprimer les autorisations offline définies pour plusieurs types de périphériques à la fois. Pour ce faire, procédez comme suit:

   a) Dans le panneau de détails, sélectionnez plusieurs types de périphériques et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Remove Offline**.

   Les autorisations adoptent alors le statut hors ligne «Use Regular» (utiliser habituel).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans DeviceLock Management Console.

Gestion des règles d'audit et de réplication hors ligne

Pour une descriptions détaillée de la fonction Auditing & Shadowing (audit et réplication), consultez le chapitre «Audit et réplication (Regular Profile).»

Les règles d'audit et de réplication hors ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les règles d'audit et de réplication ne sont pas définies pour le type de périphérique en question. Il s'agit du statut par défaut.
Configured	Indique que les règles d'audit et de réplication sont définies pour le type de périphérique en question.
No Audit	Indique une des situations suivantes: • Les droits d'audit ne sont pas définis pour tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du type de périphérique en question • Tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du type de périphériques sont supprimés. • Le compte Everyone n'a pas de droits d'audit et de réplication et est le

STATUT	DESCRIPTION
	seul compte indiqué dans les règles d'audit et de réplication pour le type de périphériques en question.
Use Regular	Indique que l'héritage des règles d'audit et de réplication hors ligne est bloqué et que les règles d'audit et de réplication habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des règles habituelles est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des règles habituelles permet d'empêcher l'application des autorisations hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur L'application des règles habituelles, consultez le chapitre intitulé «Suppression de règles d'audit et de réplication hors ligne.»

La gestion des règles d'audit et de réplication hors ligne comprend les tâches suivantes:

- Définition et édition de règles d'audit et de réplication hors ligne
- Révocation de règles d'audit et de réplication hors ligne
- Suppression de règles d'audit et de réplication hors ligne

Définition et édition de règles d'audit et de réplication hors ligne

Pour définir et éditer des règles d'audit et de réplication hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors ligne de chaque type de périphériques dans la colonne Offline (hors ligne).

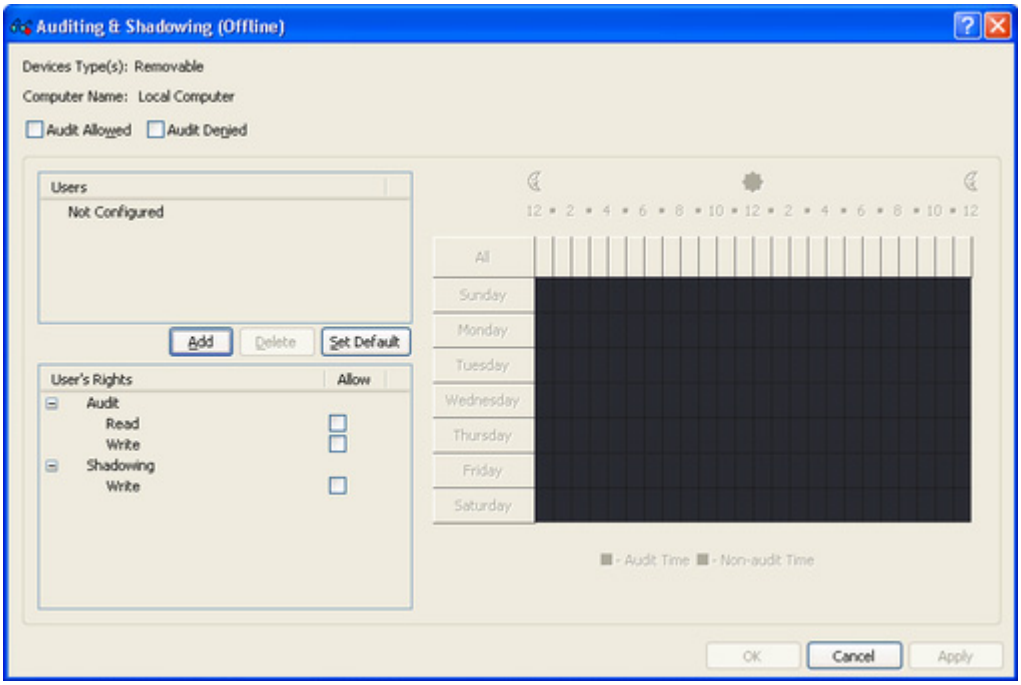
4. Dans le panneau de détails, procédez comme suit (au choix):

- Cliquez droit sur le type de périphériques pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur **Set Offline Auditing & Shadowing**.

  - OU -

- Sélectionnez le type de périphériques pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur le bouton **Set Offline Auditing & Shadowing** de la barre d'outils.

La boîte de dialogue Auditing & Shadowing (Offline) apparaît.



5. Dans la boîte de dialogue **Auditing & Shadowing (Offline)**, procédez comme suit:

POUR FAIRE CECI	PROCEDEZ COMME SUIT
Définir des règles d'audit et de réplication par défaut	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies d'accès à un périphérique. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un périphérique. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Set Default**. Les règles d'audit et de réplication par défaut s'appliquent aux membres du groupe d'utilisateurs et du compte Everyone. Pour en savoir plus sur les autorisations d'audit et de réplication définies pour ces comptes par défaut, consultez le chapitre intitulé «Audit et réplication (Regular Profile).»

POUR FAIRE CECI	PROCEDEZ COMME SUIT
Définir des règles d'audit et de réplication pour un utilisateur ou un groupe supplémentaire	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies d'accès à un périphérique. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un périphérique. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît.* 3. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Auditing & Shadowing (Offline).* 4. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue **Auditing & Shadowing (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs et/ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. 5. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Auditing & Shadowing (Offline)**, cochez ou décochez la case **Allow** située en regard des droits d'audit et de réplication appropriés. *Les droits d'audit et de réplication déterminent les actions des utilisateurs sur les périphériques qui sont répertoriées dans le journal d'audit et/ou de réplication.* *Dans le panneau de droite de la boîte de dialogue Auditing & Shadowing (Offline), vous pouvez indiquer les jours et les horaires (par exemple, de 7h00 à 17h00 du lundi au vendredi) pour lesquels les actions sur les périphériques de l'utilisateur sélectionné seront consignées dans le journal d'audit ou de réplication. Utilisez le bouton gauche de la souris pour sélectionner les jours et les horaires pour lesquels les actions sur les périphériques de l'utilisateur sélectionné seront consignées. Utilisez le bouton droit de la souris pour sélectionner les jours et les horaires pour lesquels les actions sur les périphériques de l'utilisateur sélectionné ne seront pas consignées*.
Changer des règles d'audit et de réplication pour un utilisateur ou un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'audit et de réplication appropriés.
Supprimer un utilisateur ou un groupe existant et les règles	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation de règles d'audit et de réplication hors ligne

Vous pouvez redonner aux règles d'audit et de réplication hors ligne précédemment définies le statut non configuré. Si les règles hors ligne sont non définies, les règles habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des règles d'audit et de réplication hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans Devices, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors ligne de chaque type de périphériques dans la colonne Offline (hors ligne).

4. Dans le panneau de détails, cliquez droit sur le type de périphériques pour lequel vous souhaitez révoquer les règles d'audit et de réplication hors ligne, puis cliquez sur **Undefine Offline**.

   Vous pouvez révoquer les règles d'audit et de réplication définies pour plusieurs types de périphériques à la fois. Pour ce faire, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs types de périphériques et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine Offline**.

   Le statut hors ligne des règles d'audit et de réplication passe à «Not Configured» (non configuré).

Suppression de règles d'audit et de réplication hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage des règles d'audit et de réplication hors ligne de niveau supérieur et d'appliquer les règles d'audit et de réplication habituelles pour certains groupes d'ordinateurs client de niveau inférieur. Pour que les

règles d'audit et de réplication habituelles s'appliquent, vous devez supprimer les règles d'audit et de réplication hors ligne.

Pour supprimer des règles d'audit et de réplication hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les types de périphériques pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors ligne de chaque type de périphériques dans la colonne Offline (hors ligne).
4. Dans le panneau de détails, cliquez droit sur le type de périphériques pour lequel vous souhaitez supprimer les règles d'audit et de réplication hors ligne, puis cliquez sur **Remove Offline**.

   Vous pouvez supprimer les règles d'audit et de réplication définies pour plusieurs types de périphériques à la fois. Pour ce faire, procédez comme suit:
   a) Dans le panneau de détails, sélectionnez plusieurs types de périphériques et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Remove Offline**.

   Le statut hors ligne des règles d'audit et de réplication passe à «Use Regular» (utiliser habituelles).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion de la liste blanche de périphériques USB hors ligne

Pour obtenir une description détaillée de la liste blanche de périphériques USB, consultez le chapitre intitulé «Liste blanche de périphériques USB (Regular Profile).»

La liste blanche de périphériques USB hors ligne peut avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que la liste blanche n'est pas définie. Le message suivant s'affiche: «Offline USB White List is not configured» (la liste blanche USB hors ligne n'est pas configurée). Il s'agit du statut par défaut.

STATUT	DESCRIPTION
Configured	Indique que la liste blanche est définie.
Use Regular	Indique que l'héritage de la liste blanche hors ligne est bloqué et que la liste blanche habituelle s'applique. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application de la liste blanche habituelle est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application de la liste blanche habituelle permet d'empêcher l'application de la liste blanche héritée d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application de la liste blanche habituelle, consultez le chapitre intitulé «Suppression de liste blanche de périphériques USB hors ligne.»

La gestion de la liste blanche de périphériques USB hors ligne comprend les tâches suivantes:

- Définition et édition de liste blanche de périphériques USB hors ligne
- Exportation et importation de liste blanche de périphériques USB hors ligne
- Révocation de liste blanche de périphériques USB hors ligne
- Suppression de liste blanche de périphériques USB hors ligne

Définition et édition de liste blanche de périphériques USB hors ligne

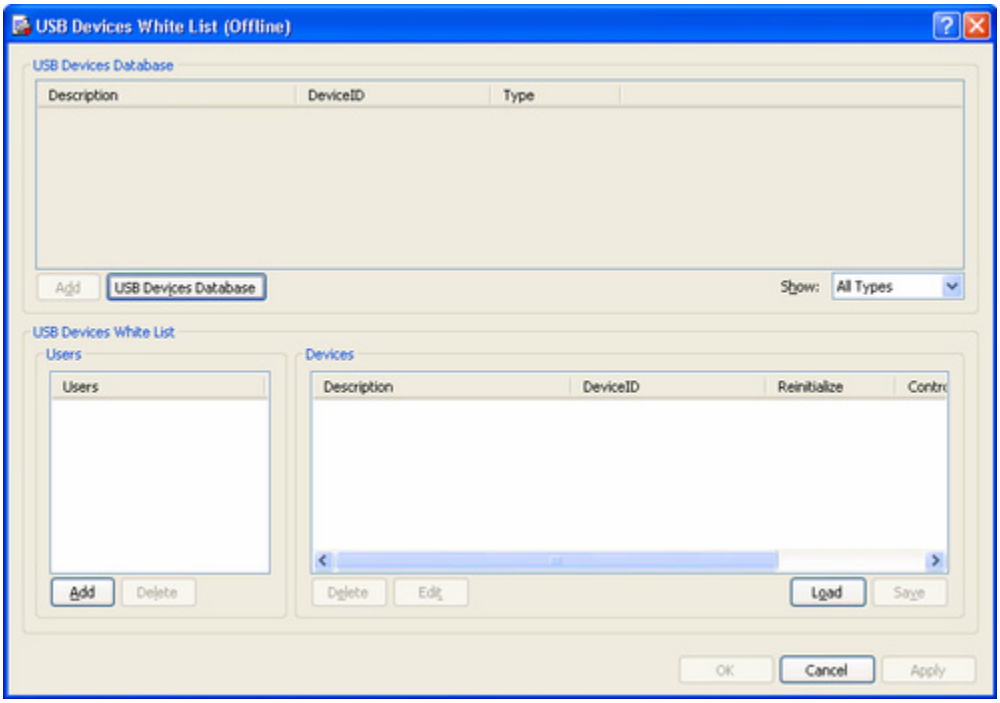
Pour définir et éditer la liste blanche de périphériques USB hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

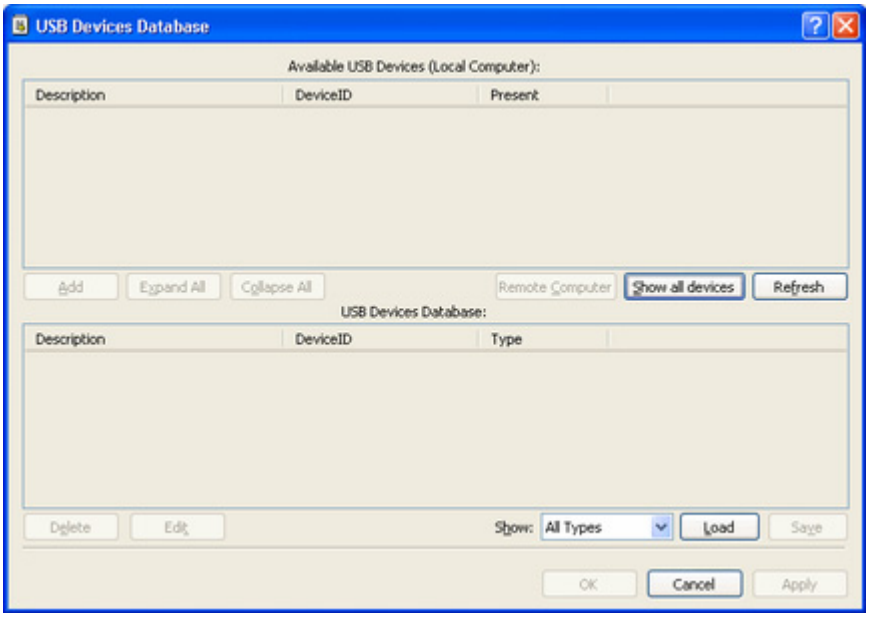
   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **USB Devices White List**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **USB Devices White List**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

La boîte de dialogue USB Devices White List (Offline) apparaît.



4. Dans le champ **USB Devices Database** du panneau supérieur de la boîte de dialogue **USB Devices White List (Offline)**, cliquez sur **USB Devices Database**.

   La boîte de dialogue USB Devices Database apparaît.



   Le champ Available USB Devices du panneau supérieur de la boîte de dialogue USB Devices Database contient une liste des périphériques connectés au moment considéré.

Pour afficher tous les périphériques connectés à un moment ou à un autre aux ports USB de l'ordinateur, cliquez sur **Show all devices**. Pour afficher tous les périphériques disponibles sur un ordinateur distant, cliquez sur **Remote Computer**.

Le bouton Remote Computer n'est pas disponible lorsque la console de gestion est connectée à l'ordinateur local.

5. Dans le champ **Available USB Devices** du panneau supérieur de la boîte de dialogue **USB Devices Database**, sélectionnez le périphérique que vous souhaitez ajouter à la liste blanche de périphériques USB, puis cliquez sur **Add**.

   Le périphérique ajouté s'affiche dans le champ USB Devices Database du panneau inférieur de la boîte de dialogue.

   Remarque: Vous ne pourrez ajouter un périphérique à la liste blanche de périphériques USB qu'après l'avoir ajouté à la base de périphériques USB.

   La même base de périphériques USB est utilisée pour les listes blanches de périphériques USB habituelle et hors ligne.

   Pour supprimer un périphérique de la base de périphériques USB, procédez comme suit dans le champ **USB Devices Database** du panneau inférieur de la boîte de dialogue **USB Devices Database**:

   - Sélectionnez le périphérique, puis cliquez sur **Delete**.
     - OU -
   - Cliquez droit sur le périphérique, puis cliquez sur **Delete**.

   Les périphériques ne sont pas supprimés automatiquement de la liste blanche une fois supprimés de la base de périphériques USB.

   Pour modifier la description d'un périphérique, sélectionnez-le dans le champ **USB Devices Database** du panneau inférieur de la boîte de dialogue **USB Devices Database**, puis cliquez sur **Edit**.

   Si vous changez la description d'un périphérique dans la base de périphériques USB, le périphérique en question figurera dans la liste blanche avec son ancienne description en cas d'ajout à la liste blanche.

6. Cliquez sur **OK** ou sur **Apply**.

   Le périphérique ajouté à la base de périphériques USB s'affiche dans le champ USB Devices Database du panneau supérieur de la boîte de dialogue USB Devices White List (Offline).

7. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **USB Devices White List (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

8. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la liste blanche de périphériques USB, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau supérieur gauche de la boîte de dialogue USB Devices White List (Offline).

   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **USB**

Devices White List (Offline), puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

9. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **USB Devices White List (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

10. Dans le champ **USB Devices Database** du panneau supérieur de la boîte de dialogue **USB Devices White List (Offline)**, sélectionnez le périphérique que vous souhaitez ajouter à la liste blanche de l'utilisateur ou du groupe sélectionné, puis cliquez sur **Add**.

    Pour sélectionner plusieurs périphériques, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

    Les périphériques ajoutés à la liste blanche s'affichent dans le champ Devices du panneau inférieur droit de la boîte de dialogue.

    Pour supprimer un périphérique de la liste blanche de l'utilisateur ou du groupe sélectionné, procédez comme suit dans le champ **Devices** de la boîte de dialogue **USB Devices White List (Offline)**:

    - Sélectionnez le périphérique, puis cliquez sur **Delete**.
      - OU -
    - Cliquez droit sur le périphérique, puis cliquez sur **Delete**.
      - OU -
    - Sélectionnez le périphérique, puis cliquez sur la touche Delete.

    Pour modifier la description d'un périphérique, procédez comme suit dans le champ **Devices** du panneau inférieur droit de la boîte de dialogue **USB Devices White List (Offline)**:

    - Sélectionnez le périphérique, puis cliquez sur **Edit**.
      - OU -
    - Cliquez droit sur le périphérique, puis cliquez sur **Edit**.

11. Cliquez sur **OK** ou sur **Apply**.

Exportation et importation de liste blanche de périphériques USB hors ligne

Vous pouvez exporter la liste blanche de périphériques USB hors ligne à un fichier .whl que vous pouvez importer et utiliser sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter la liste blanche de périphériques USB hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.

b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **USB Devices White List**, puis cliquez sur **Save Offline**.
     - OU -
   - Sélectionnez **USB Devices White List**, puis cliquez sur l'option **Save Offline** de la barre d'outils.
     - OU -
   - Développez **USB Devices White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Save Offline**.
     - OU -
   - Développez **USB Devices White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur le périphérique indiqué dans la liste blanche, puis cliquez sur **Save**.
     - OU -
   - Cliquez droit sur **USB Devices White List**, puis cliquez sur **Manage Offline**. Dans le champ **Devices** du panneau inférieur droit de la boîte de dialogue **USB Devices White List (Offline)**, cliquez sur **Save**.

   La boîte de dialogue Save As apparaît.

4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .whl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez la liste blanche de périphériques USB hors ligne, celle-ci est sauvegardée dans un fichier doté d'une extension .whl.

Pour importer la liste blanche de périphériques USB hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **USB Devices White List**, puis cliquez sur **Load Offline**.
     - OU -
   - Sélectionnez **USB Devices White List**, puis cliquez sur l'option **Load Offline** de la barre d'outils.
     - OU -
   - Développez **USB Devices White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Load Offline**.
     - OU -
   - Développez **USB Devices White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur le périphérique indiqué dans la liste blanche, puis cliquez sur **Load**.
     - OU -
   - Cliquez droit sur **USB Devices White List**, puis cliquez sur **Manage Offline**. Dans le champ Devices du panneau inférieur droit de la boîte de dialogue **USB Devices White List (Offline)**, cliquez sur **Load**.

   La boîte de dialogue Open apparaît.

4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrer le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

Révocation de liste blanche de périphériques USB hors ligne

Vous pouvez redonner à la liste blanche hors ligne précédemment définie le statut non configurée. Si la liste blanche hors ligne est indéfinie, la liste blanche habituelle s'applique aux ordinateurs client hors ligne.

Pour révoquer la liste blanche de périphériques USB hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Cliquez droit sur l'option **USB Devices White List** du champ **Devices**, puis cliquez sur **Undefine Offline**.

   Le statut hors ligne de la liste blanche passe à «Not Configured» (non configuré).

   Lorsque vous sélectionnez USB Devices White List dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline USB White List is not configured.» (la liste blanche USB hors ligne n'est pas configurée)

Suppression de liste blanche de périphériques USB hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage de la liste blanche hors ligne de niveau supérieur et d'appliquer la liste blanche habituelle à certains groupes d'ordinateurs client de niveau inférieur. Pour que la liste blanche de périphériques USB habituelle s'applique, vous devez supprimer la liste blanche de périphériques hors ligne.

Pour supprimer la liste blanche de périphériques USB hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Cliquez droit sur l'option **USB Devices White List** du champ **Devices**, puis cliquez sur **Remove Offline**.

   Le statut hors ligne de la liste blanche passe à «Use Regular» (utiliser habituel).

   Lorsque vous sélectionnez USB Devices White List dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline USB White List is configured to use Regular USB White List» (la liste blanche USB hors ligne est configurée pour utiliser la liste blanche USB habituelle).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans DeviceLock Management Console.

Gestion de la liste blanche de médias hors ligne

Pour obtenir une description détaillée de la liste blanche de médias, veuillez consulter le chapitre intitulé «Liste blanche de médias (Regular Profile).»

La liste blanche de médias hors ligne peut avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que la liste blanche n'est pas définie. Le message suivant s'affiche: «Offline Media List is not configured.» (la liste blanche de médias hors ligne n'est pas configurée) Il s'agit du statut par défaut.
Configured	Indique que la liste blanche est définie.
Use Regular	Indique que l'héritage de la liste blanche hors ligne est bloqué et que la liste blanche habituelle s'applique. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application de la liste blanche habituelle est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application de la liste blanche habituelle permet d'empêcher l'application de la liste blanche héritée d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application de la liste blanche habituelle, consultez le chapitre intitulé «Suppression de liste blanche de médias hors ligne.»

La gestion de la liste blanche de médias hors ligne comprend les tâches suivantes:

- Définition et édition de liste blanche de médias hors ligne
- Exportation et importation de liste blanche de médias hors ligne
- Révocation de liste blanche de médias hors ligne
- Suppression de liste blanche de médias hors ligne

Définition et édition de liste blanche de médias hors ligne

Pour définir et éditer la liste blanche de médias hors ligne

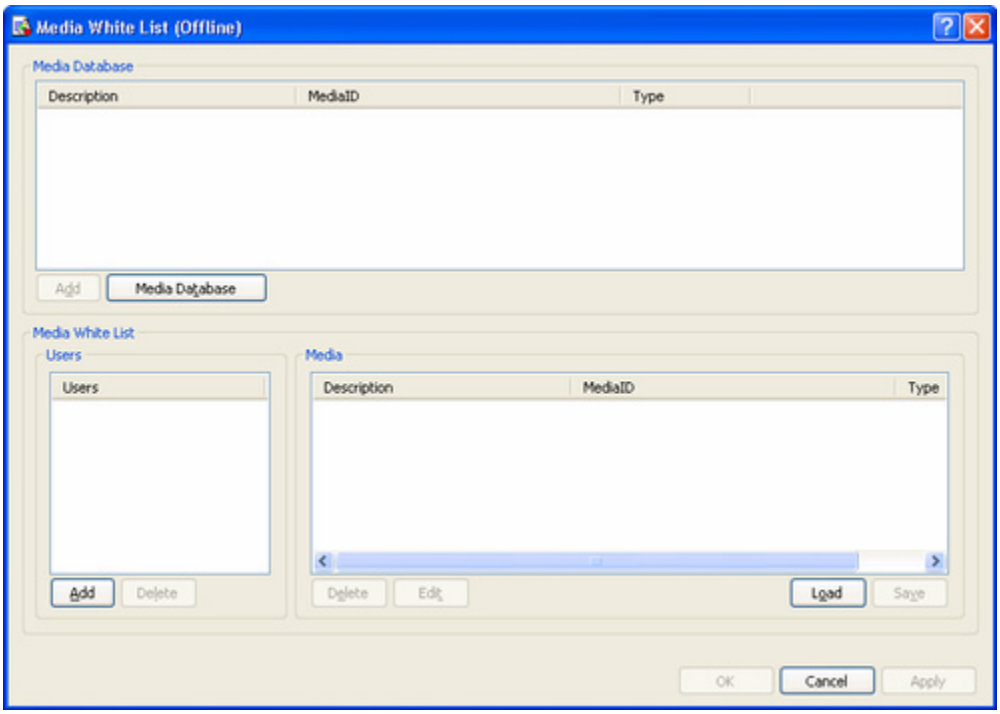
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Media White List**, puis cliquez sur **Manage Offline**.
     - OU -

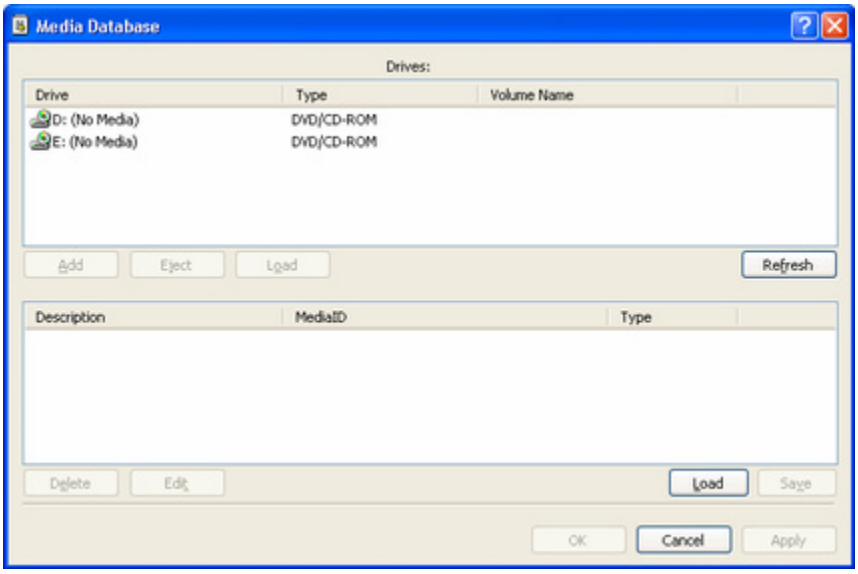
- Sélectionnez **Media White List**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

La boîte de dialogue Media White List (Offline) apparaît.



4. Dans le champ **Media Database** du panneau supérieur de la boîte de dialogue **Media White List (Offline)**, cliquez sur **Media Database**.

La boîte de dialogue Media Database apparaît.



Le champ Drives du panneau supérieur de la boîte de dialogue Media Database contient une liste de tous les lecteurs de CD-ROM et DVD-ROM disponibles sur l'ordinateur local.

*La liste de ces lecteurs est automatiquement mise à jour et elle affiche immédiatement les nouveaux médias. Pour mettre à jour cette liste manuellement, cliquez sur **Refresh**.*

5. Dans le champ **Drives** du panneau supérieur de la boîte de dialogue **Media Database**, sélectionnez le lecteur qui contient le média que vous souhaitez ajouter à la liste blanche de médias, puis cliquez sur **Add**.

   Les médias sélectionnés sont ajoutés à la base de médias et figurent dans le panneau inférieur de la boîte de dialogue Media Database.

   Remarque: Vous ne pouvez ajouter des médias à la liste blanche de médias qu'après les avoir ajoutés à la base de médias.

   La même base de médias est utilisée pour les listes blanches de médias habituelle et hors ligne.

   Pour supprimer un média de la liste blanche, procédez comme suit dans le panneau inférieur de la boîte de dialogue **Media Database**:

   - Sélectionnez le média, puis cliquez sur **Delete**.
     - OU -
   - Cliquez droit sur le média, puis cliquez sur **Delete**.

   Pour modifier la description d'un média, sélectionnez-le dans le panneau inférieur de la boîte de dialogue **Media Database**, puis cliquez sur **Edit**.

6. Cliquez sur **OK** ou sur **Apply**.

   Les média ajoutés à la base de médias s'affichent dans le champ Media Database du panneau supérieur de la boîte de dialogue Media White List (Offline).

7. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Media White List (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

8. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la liste blanche de médias, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau inférieur gauche de la boîte de dialogue Media White List (Offline).

   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Media White List (Offline)**, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

9. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Media White List (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

10. Dans le champ **Media Database** du panneau supérieur de la boîte de dialogue **Media White List (Offline)**, sélectionnez le média que vous souhaitez ajouter à la liste blanche de l'utilisateur ou du groupe sélectionné, puis cliquez sur **Add**.

Pour sélectionner plusieurs médias, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

Les médias ajoutés à la liste blanche s'affichent dans le champ Media du panneau inférieur droit de la boîte de dialogue.

Pour supprimer un média de la liste blanche de l'utilisateur ou du groupe sélectionné, procédez comme suit dans le champ **Media** de la boîte de dialogue **Media White List (Offline)**:

- Sélectionnez le média, puis cliquez sur **Delete**.
  - OU -
- Cliquez droit sur le média, puis cliquez sur **Delete**.

Pour modifier la description d'un média de l'utilisateur ou du groupe sélectionné, procédez comme suit dans le champ **Media** de la boîte de dialogue **Media White List (Offline)**:

- Sélectionnez le média, puis cliquez sur **Edit**.
  - OU -
- Cliquez droit sur le média, puis cliquez sur **Edit**.

11. Cliquez sur **OK** ou sur **Apply**.

Exportation et importation de liste blanche de médias hors ligne

Vous pouvez exporter la liste blanche de médias hors ligne à un fichier .mwl que vous pouvez importer et utiliser sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter la liste blanche de médias hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Media White List**, puis cliquez sur **Save Offline**.
     - OU -
   - Sélectionnez **Media White List**, puis cliquez sur l'option **Save Offline** de la barre d'outils.
     - OU -

- Développez **Media White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Save Offline**.
  - OU -
- Développez **Media White List**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur le média indiqué dans la liste blanche, puis cliquez sur **Save**.
  - OU -
- Cliquez droit sur **Media White List**, puis cliquez sur **Manage Offline**. Dans le champ **Media** du panneau inférieur droit de la boîte de dialogue **Media White List (Offline)**, cliquez sur **Save**.

La boîte de dialogue Save As apparaît.

4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .mwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez la liste blanche de médias hors ligne, celle-ci est sauvegardée dans un fichier doté d'une extension .mwl.

Pour importer la liste blanche de médias hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Media White List**, puis cliquez sur **Load Offline**.
     - OU -
   - Sélectionnez **Media White List**, puis cliquez sur l'option **Load Offline** de la barre d'outils.
     - OU -
   - Développez **Media White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Load Offline**.
     - OU -
   - Développez **Media White List**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de

détails, cliquez droit sur le périphérique indiqué dans la liste blanche, puis cliquez sur **Load**.

- OU -

- Cliquez droit sur **Media White List**, puis cliquez sur **Manage Offline**. Dans le champ **Media** du panneau inférieur droit de la boîte de dialogue **Media White List (Offline)**, cliquez sur **Load**.

La boîte de dialogue Open apparaît.

4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrer le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

Révocation de liste blanche de médias hors ligne

Vous pouvez redonner à la liste blanche hors ligne précédemment définie le statut non configuré. Si la liste blanche hors ligne est indéfinie, la liste blanche habituelle s'applique aux ordinateurs client hors ligne.

Pour révoquer la liste blanche de médias hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Cliquez droit sur l'option **Media White List** du champ **Devices**, puis cliquez sur **Undefine Offline**.

   La liste blanche adopte alors le statut hors liste «Not Configured» (non configuré).

   Lorsque vous sélectionnez Media White List dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Media List is not configured» (La liste blanche de médias hors ligne n'est pas configurée).

Suppression de liste blanche de médias hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage de la liste blanche hors ligne de niveau supérieur et d'appliquer la liste blanche habituelle à certains groupes

d'ordinateurs client de niveau inférieur. Pour que la liste blanche de médias habituelle s'applique, vous devez supprimer la liste blanche de périphériques hors ligne.

Pour supprimer la liste blanche de médias hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Cliquez droit sur l'option **Media White List** du champ **Devices**, puis cliquez sur **Remove Offline**.

   Le statut hors ligne de la liste blanche passe à «Use Regular» (utiliser habituel).

   Lorsque vous sélectionnez **Media White List** dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Media White List is configured to use Regular Media White List» (La liste blanche de médias hors ligne est configurée pour utiliser la liste blanche de médias habituelle).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans DeviceLock Management Console.

Gestion des règles contextuelles hors ligne pour les périphériques

Pour une description détaillée de la fonction Content-Aware Rules (règles contextuelles) pour les périphériques, consultez le chapitre «Règles contextuelles pour les périphériques (Regular Profile).»

Les règles contextuelles hors ligne peuvent avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les règles contextuelles ne sont pas définies. Le message suivant s'affiche : «Offline Content-Aware Rules are not configured» (Les règles contextuelles hors ligne ne sont pas configurées). Il s'agit du statut par défaut.
Configured	Indique que les règles contextuelles sont définies.
Use Regular	Indique que l'héritage des règles contextuelles hors ligne est bloqué et que les règles contextuelles habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des règles contextuelles habituelles est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des règles contextuelles habituelles permet d'empêcher l'application des règles contextuelles hors ligne héritées d'un niveau supérieur à un groupe spécifique

STATUT	DESCRIPTION
	d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des règles contextuelles habituelles, consultez le chapitre intitulé «Suppression de règles contextuelles hors ligne.»

La gestion des règles contextuelles hors ligne comprend les tâches suivantes:

- Définition de règles contextuelles hors ligne
- Modification de règles contextuelles hors ligne
- Copie de règles contextuelles hors ligne
- Exportation et importation de règles contextuelles hors ligne
- Suppression de règles contextuelles hors ligne
- Révocation de règles contextuelles hors ligne
- Suppression de règles contextuelles hors ligne

Définition de règles contextuelles hors ligne

Les règles contextuelles sont créées sur la base des groupes de contenus intégrés ou sur la base des groupes de contenus personnalisés. Pour plus d'informations sur ces groupes, voir «Configuration des paramètres de détection de contenu.»

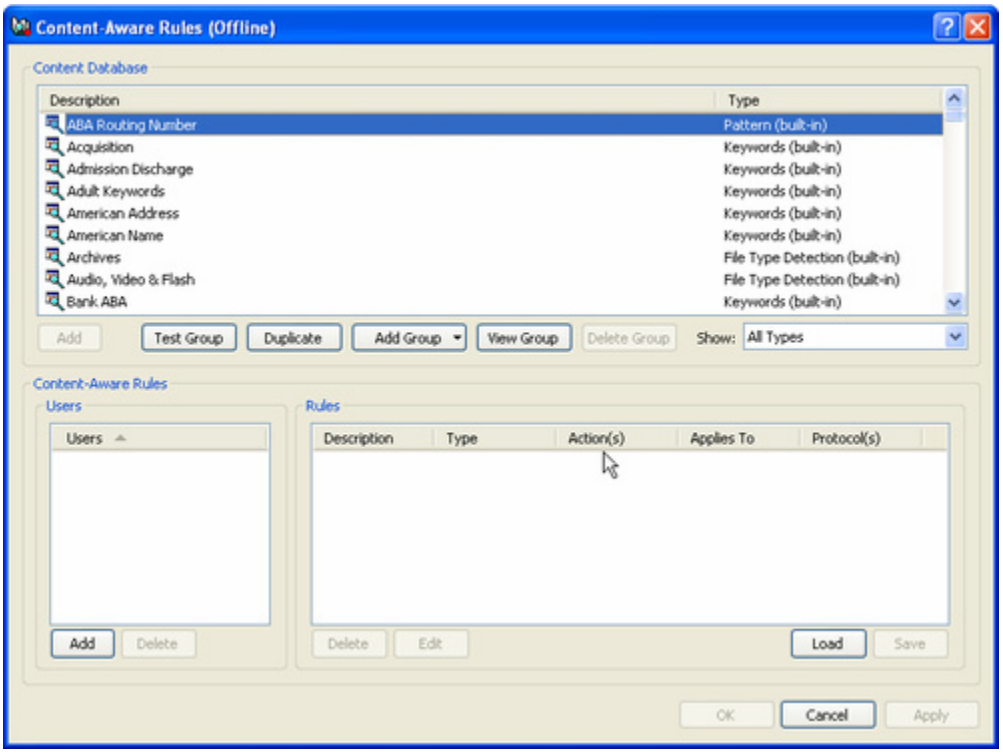
Pour définir une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules (Offline) apparaît.



4. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau inférieur gauche de la boîte de dialogue Content-Aware Rules (Offline).

   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

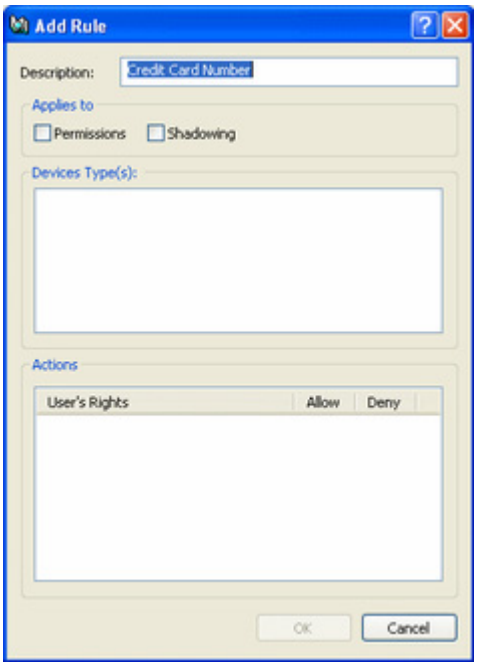
6. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez les utilisateurs ou les groupes pour lesquels vous souhaitez définir la règle.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez le groupe de contenus souhaité, puis cliquez sur **Add**.

   Remarque: Vous ne pouvez indiquer qu'un seul groupe de contenus par règle contextuelle.

   La boîte de dialogue Add Rule apparaît.



8. Dans le champ **Description** de la boîte de dialogue **Add Rule**, saisissez le nom de la règle contextuelle.

   Par défaut, la règle contextuelle a le même nom que le groupe de contenus indiqué mais vous pouvez saisir un nom différent.

9. Dans le champ **Applies to**, indiquez le type d'opération associé à la règle. Les options disponibles sont les suivantes:
   - **Permissions**: Indique que la règle s'appliquera aux opérations de contrôle d'accès.
   - **Shadowing**: Indique que la règle s'appliquera aux opérations de copie de réplication.
   - **Permissions**, **Shadowing**: Indique que la règle s'appliquera aux opérations de contrôle d'accès et de copie de réplication.

10. Dans **Device Type(s)**, sélectionnez le ou les types de périphériques auxquels vous souhaitez que cette règle s'applique.

    Les règles contextuelles peuvent s'appliquer aux périphériques de types DVD/CD-ROM, Floppy, Palm, Removable et Windows Mobile.

11. Dans le champ **Action(s)**, indiquez les actions utilisateur qui sont autorisées ou non sur les fichiers, et celles qui sont consignées dans le journal de réplication.

    Vous pouvez sélectionner l'une ou l'autre des options suivantes: Read, Write, Read and Write.

    Si la règle s'applique aux copies de réplication ou à la fois au contrôle d'accès et aux copies de réplication, l'option Read est accessible. Pour en savoir plus sur les droits d'utilisateur susceptibles d'être indiqués dans les règles contextuelles, consultez les chapitres intitulés «Règles contextuelles pour opérations de contrôle d'accès» et «Règles contextuelles pour opération de copie de réplication.»

12. Cliquez sur **OK**.

    La règle ainsi créée figure dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules (Offline).

13. Cliquez sur **OK** ou **Apply** pour appliquer la règle.

    Les utilisateurs ou les groupes auxquels s'applique la règle contextuelle figurent dans la section Content-Aware Rules de l'arborescence.

    Si vous sélectionnez un utilisateur ou un groupe auquel la règle contextuelle s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

    - **Description** Le nom de la règle. Par défaut, la règle a le même nom que le groupe de contenus indiqué.
    - **Type** Le type de l'analyse de contenus. Valeurs possibles: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, et **Complex**. **File Type Detection** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs signatures propres. **Keywords** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des mots clés et des expressions spécifiés. **Pattern** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des modèles de textes décrits par les expressions régulières Perl. **Document Properties** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs propriétés. **Complex** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction du contenu décrit par une expression booléenne.
    - **Action(s)** Indique les actions utilisateur qui sont autorisées ou non sur les fichiers, et celles qui sont consignées dans le journal de réplication.
    - **Applies To** Valeurs possibles: **Permissions**, **Shadowing**, et **Permissions, Shadowing**. **Permissions** indique que la règle s'applique aux contrôles d'accès. **Shadowing** indique que la règle s'applique aux copies de réplication. **Permissions, Shadowing** indique que la règle s'applique à la fois aux contrôles d'accès et aux copie de réplication.
    - **Device Type(s)** Les types de périphériques auxquels s'applique la règle.
    - **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs client qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs client qui travaillent hors ligne.

      Vous pouvez définir des règles contextuelles différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur la façon de définir les règles contextuelles en ligne, consultez le chapitre intitulé «Gestion des règles contextuelles.»

Modification de règles contextuelles hors ligne

Vous pouvez modifier les propriétés des règles contextuelles comme Description, Applies To, Device Type(s), Actions.

Pour modifier une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

a) Ouvrez DeviceLock Service Settings Editor.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, cliquez droit sur **Content-Aware Rules**, cliquez sur **Manage Offline**, puis procédez comme suit:

   a) Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles auxquelles ils sont soumis dans l'option Rules du panneau inférieur droit de la boîte de dialogue.

   b) Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.

   - OU -

   Cliquez droit sur la règle, puis cliquez sur **Edit**.

   - OU -

   Dans **Devices**, développez **Content-Aware Rules**, puis procédez comme suit:

   a) Dans **Content-Aware Rules**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles auxquelles ils sont soumis dans le panneau de détails.

   b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.

   La boîte de dialogue Edit Rule apparaît.

4. Dans la boîte de dialogue **Edit Rule**, modifiez les propriétés des règles en fonction de vos besoins.
5. Cliques sur **OK** pour valider les modifications.

Copie de règles contextuelles hors ligne

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles contextuelles hors ligne existantes.

Pour copier une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules (Offline) apparaît.
4. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle que vous souhaitez copier.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles auxquelles ils sont soums dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
5. Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez droit sur la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

   La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

   Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Lorsque vous coupez la règle, celle-ci ne sera coupée qu'une fois collée.

   Pour effectuer un glisser/déposer, sélectionnez la règle et déplacez-la sur l'utilisateur ou le groupe d'utilisateurs auxquels vous désirez appliquer la règle ainsi copiée.
6. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.
7. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes auxquels s'applique la règle que vous souhaitez copier, puis cliquez sur **OK**.

Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau inférieur gauche de la boîte de dialogue Content-Aware Rules (Offline).

8. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez définir des autorisations.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

9. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez droit dans le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée figure dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules (Offline).

10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de règles contextuelles hors ligne

Vous pouvez exporter toutes vos règles contextuelles en cours dans un fichier .cwl susceptible d'être importé et utilisé sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Save Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Save Offline** de la barre d'outils.
     - OU -
   - Développez **Content-Aware Rules**, cliquez droit sur n'importe quel utilisateur ou groupe, puis cliquez sur **Save Offline**.
     - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Save**.
  - OU -
- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Save Offline** de la barre d'outils.
  - OU -
- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage (Offline)**. Dans le champ **Users** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Save**.

La boîte de dialogue Save As apparaît.

4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .cwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez des règles, celles-ci sont sauvegardées dans un fichier à extension .cwl.

Pour importer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Load Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Load Offline** de la barre d'outils.
     - OU -
   - Développez **Content-Aware Rules**, cliquez droit sur n'importe quel utilisateur ou groupe, puis cliquez sur **Load Offline**.
     - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Load**.

  - OU -

- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Load Offline** de la barre d'outils.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**. Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Load**.

La boîte de dialogue Open apparaît.

4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Vous ne pouvez importer qu'un seul fichier .cwl à la fois.

Suppression de règles contextuelles hors ligne

Vous pouvez supprimer les règles contextuelles hors ligne individuelles qui ne sont plus nécessaires.

Pour supprimer une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Développez **Content-Aware Rules**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.

     Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.

     - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.

  Pour sélectionner plusieurs règles à supprimer, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

Révocation de règles contextuelles hors ligne

Vous pouvez redonner aux règles contextuelles hors ligne précédemment définies le statut non configuré. Si les règles hors ligne sont non définies, les règles habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez DeviceLock Service.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez DeviceLock Service.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Undefine Offline**.

   Les règles contextuelles adopte alors le statut hors ligne «Not Configured» (non configuré).

   Lorsque vous sélectionnez **Content-Aware Rules** dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Content-Aware Rules are not configured» (Les règles contextuelles hors ligne ne sont pas configurées).

Suppression de règles contextuelles hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer les règles contextuelles hors ligne héritées d'un niveau supérieur et d'appliquer les règles contextuelles habituelles à certains

groupes d'ordinateurs client de niveau inférieur. Pour que les règles contextuelles habituelles s'appliquent, vous devez supprimer les règles contextuelles hors ligne.

Pour supprimer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Remove Offline**.

   Les règles contextuelles adoptent alors le statut hors ligne «Use Regular» (utiliser habituelles).

   Lorsque vous sélectionnez **Content-Aware Rules** dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Content-Aware Rules are configured to use Regular Content-Aware Rules» (Les règles contextuelles hors ligne sont configurées pour utiliser les règles contextuelles habituelles).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion des paramètres de sécurité hors ligne

Pour une descriptions détaillée de la fonction Security Settings, consultez le chapitre «Paramètres de sécurité (Regular Profile).»

Les paramètres de sécurité hors ligne peuvent avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les paramètres de sécurité hors ligne ne sont pas définis. Il s'agit du statut par défaut.
Enabled	Indique que les paramètres de sécurité hors ligne sont définis pour permettre le contrôle d'audit et d'accès aux catégories de périphériques indiquées.
Disabled	Indique que les paramètres de sécurité hors ligne sont définis pour désactiver le contrôle d'audit et d'accès aux catégories de périphériques indiquées.
Use Regular	Indique que l'héritage des paramètres de sécurité hors ligne est bloqué et que les paramètres de sécurité habituels s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des paramètres de sécurité habituels est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des

STATUT	DESCRIPTION
	paramètres de sécurité habituels permet d'empêcher l'application des paramètres de sécurité hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des paramètres de sécurité habituels, consultez le chapitre intitulé «Suppression de paramètres de sécurité hors ligne.»

La gestion des paramètres de sécurité hors ligne comprend les tâches suivantes:

- Définition et modification de paramètres de sécurité hors ligne
- Révocation de paramètres de sécurité hors ligne
- Suppression de paramètres de sécurité hors ligne

Définition et modification de paramètres de sécurité hors ligne

Les paramètres de sécurité hors ligne peuvent être définis et modifiés de façon individuelle ou collective.

Pour définir et modifier des paramètres de sécurité hors ligne de façon individuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Security Settings**.

   Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
4. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité, puis cliquez sur **Enable Offline**.

   Le paramètre de sécurité passe du statut hors ligne «Not Configured» au statut hors ligne «Enabled».

   Une fois un paramètre de sécurité particulier activé, vous pouvez le désactiver. Pour ce faire, cliquez droit sur le paramètre de sécurité activé, puis clique sur **Disable Offline**.

   Le paramètre de sécurité passe du statut hors ligne «Enabled» au statut hors ligne «Disabled».

Pour définir et modifier des paramètres de sécurité hors ligne de façon collective

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

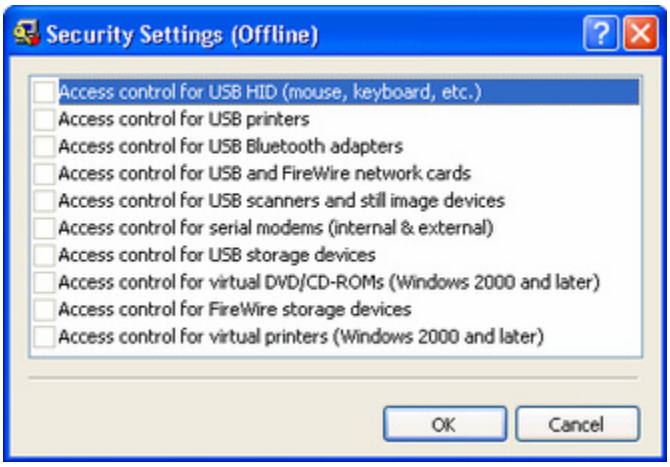
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:

   - Cliquez droit sur **Security Settings**, puis cliquez sur **Manage Offline**.
     - OU –
   - Sélectionnez **Security Settings**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.
     - OU -
   - Sélectionnez **Security Settings**. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité, puis cliquez sur **Manage Offline**.
     - OU –
   - Sélectionnez **Security Settings**. Dans le panneau de détails, sélectionnez n'importe quel paramètre de sécurité, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

     Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.

   La boîte de dialogue Security Settings (Offline) apparaît.


Security Settings (Offline)
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual DVD/CD-ROMs (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
OK
Cancel

4. Dans la boîte de dialogue **Security Settings (Offline)**, cochez les cases des paramètres de sécurité que vous souhaitez définir.

Une fois des paramètres de sécurité activés, vous pouvez les désactiver. Pour ce faire, décochez les cases correspondantes.

Remarque: Toutes les case de la boîte de dialogue **Security Settings (Offline)** ont trois statuts: coché, décoché et indéterminé qui correspondent aux statuts Enabled (activé), Disabled (désactivé) et Not Configured (non configuré) des paramètres de sécurité.

5. Cliquez sur **OK**.

Révocation de paramètres de sécurité hors ligne

Vous pouvez redonner aux paramètres de sécurité hors ligne précédemment définis le statut non configuré. Si les paramètres de sécurité hors ligne sont non définis, les paramètres de sécurité habituels s'appliquent aux ordinateurs client hors ligne. Vous pouvez révoquer les paramètres de sécurité de façon individuelle ou collective.

Pour révoquer les paramètres de sécurité de façon individuelle

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Security Settings**.

   Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
4. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité à révoquer, puis cliquez sur **Undefine Offline**.

   Le paramètre de sécurité adopte alors le statut hors ligne «Not Configured» (non configuré).

Pour révoquer les paramètres de sécurité de façon collective

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.

b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Security Settings**, puis cliquez sur **Manage Offline**.
     - OU –
   - Sélectionnez **Security Settings**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.
     - OU -
   - Sélectionnez **Security Settings**. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité, puis cliquez sur **Manage Offline**.
     - OU –
   - Sélectionnez **Security Settings**. Dans le panneau de détails, sélectionnez n'importe quel paramètre de sécurité, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

     Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.

   La boîte de dialogue Security Settings (Offline) apparaît.

4. Dans la boîte de dialogue **Security Settings (Offline)**, remettez les cases appropriées en mode indéterminé.

Remarque: Toutes les case de la boîte de dialogue **Security Settings (Offline)** ont trois statuts: coché, décoché et indéterminé qui correspondent aux statuts Enabled (activé), Disabled (désactivé) et Not Configured (non configuré) des paramètres de sécurité.

Suppression de paramètres de sécurité hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer les paramètres de sécurité hors ligne hérités d'un niveau supérieur et d'appliquer les paramètres de sécurité habituels à certains groupes d'ordinateurs client de niveau inférieur. Pour que les paramètres de sécurité habituels s'appliquent, vous devez supprimer les paramètres de sécurité hors ligne. La suppression des paramètres de sécurité ne peut se faire que de façon individuelle.

Pour supprimer des paramètres de sécurité hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Devices**.
3. Dans **Devices**, sélectionnez **Security Settings**.

   Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.

4. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité à supprimer, puis cliquez sur **Remove Offline**.

   Le paramètre de sécurité adopte alors le statut hors ligne «Use Regular».

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion des politiques de sécurité hors ligne pour les protocoles

La gestion des politiques de sécurité hors ligne pour les protocoles comprend les opérations suivantes:

- Gestion des autorisations hors ligne pour les protocoles
- Gestion des règles d'audit et de réplication hors ligne pour les protocoles
- Gestion de la liste blanche de protocoles hors ligne
- Gestion des règles contextuelles hors ligne pour les protocoles
- Gestion des paramètres de sécurité hors ligne pour les protocoles

Gestion des autorisations hors ligne pour les protocoles

Pour une description détaillée de la fonction Permissions (autorisations) pour les protocoles, consultez le chapitre «Gestion d'autorisations pour les protocoles.»

Les autorisations hors ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les autorisations ne sont pas définies. Il s'agit du statut par défaut.
Configured	Indique que les autorisations sont définies.
Full Access	Indique que le compte Everyone (tout le monde) bénéficie de tous les droits d'accès.
No Access	Indique une des situations suivantes: • Le compte Everyone (tout le monde) bénéficie d'autorisations No Access (pas d'accès) et est le seul compte assigné à un protocole. *Les autorisations No Access (pas d'accès) assignées au compte Everyone (tout le monde) l'emportent sur les autorisations assignées aux autres*

STATUT	DESCRIPTION
	comptes. • Tous les utilisateurs et les groupes assignés à un protocole bénéficient d'autorisations No Access (pas d'accès). • Tous les utilisateurs et les groupes assignés à un protocole sont supprimés.
Use Regular	Indique que l'héritage des autorisations hors ligne est bloqué et que les autorisations habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des autorisations habituelles est utile si vous utilisez les fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des autorisations habituelles permet d'empêcher l'application des autorisations hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des autorisations habituelles, consultez le chapitre intitulé «Suppression d'autorisations hors ligne.»

La gestion des autorisations hors ligne comprend les tâches suivantes:

- Définition et édition d'autorisations hors ligne
- Révocation d'autorisations hors ligne
- Suppression d'autorisations hors ligne

Définition et édition d'autorisations hors ligne

Pour définir et éditer des autorisations hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

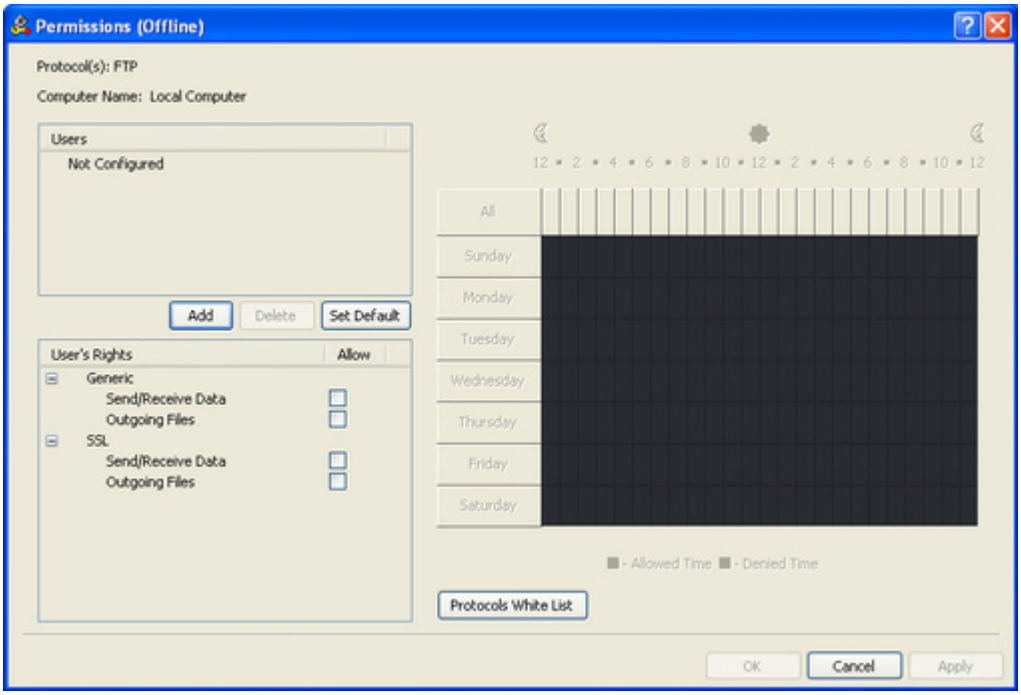
   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque protocole dans la colonne Offline (hors ligne).

4. Dans le panneau de détails, procédez comme suit:
   - Cliquez droit sur le protocole pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur **Set Offline Permissions**.
     - - OU -
   - Sélectionnez le protocole pour lequel vous souhaitez définir ou éditer des autorisations, puis cliquez sur le bouton **Set Offline Permissions** de la barre d'outils.

   La boîte de dialogue Permissions (Offline) apparaît.



5. Dans la boîte de dialogue **Permissions (Offline)**, procédez comme suit:

ACTION	PROCEDURE
Définir des autorisations par défaut	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Set Default**. *Les autorisations par défaut sont assignées aux comptes Administrators et Everyone. Pour en savoir plus sur les autorisations définies pour ces comptes par défaut, consultez le chapitre intitulé* «Gestion des autorisations de protocoles.»
Définir des autorisations pour un utilisateur ou un groupe supplémentaire	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît*. 2. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes ajoutés figurent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Permissions (Offline).* 3. Dans le champ **Users** du panneau supérieur gauche de la boîte

ACTION	PROCEDURE
	de dialogue **Permissions (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs et/ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. 4. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Permissions (Offline)**, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés. *Le panneau de droite de la boîte de dialogue Permissions (Offline) permet de définir les limites d'accès des utilisateurs aux protocoles en termes de jours et d'heures. Utilisez le bouton gauche de la souris pour sélectionner les jours et les horaires pendant lesquels l'utilisateur ou le groupe sélectionné aura accès aux protocoles. Utilisez le bouton droit de la souris pour indiquer les jours et les horaires pendant lesquels l'utilisateur ou le groupe sélectionné n'aura pas accès aux protocoles*.
Changer les autorisations d'un utilisateur ou d'un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés.
Supprimer un utilisateur ou un groupe existant et ses autorisations	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation d'autorisations hors ligne

Vous pouvez redonner aux autorisations hors ligne précédemment définies le statut non configuré. Si les autorisations hors ligne sont non définies, les autorisations habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des autorisations hors lignes

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.

b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque protocole dans la colonne Offline (hors ligne).

4. Dans le panneau de détails, cliquez droit sur le protocole pour lequel vous souhaitez révoquer les autorisations hors ligne, puis cliquez sur **Undefine Offline**.

   Vous pouvez révoquer les autorisations hors ligne de plusieurs protocoles en même temps. Pour ce faire, procédez comme suit:

   a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine Offline**.

   Les autorisations adoptent alors le statut hors ligne «Not Configured» (non configuré).

Suppression d'autorisations hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage des autorisations hors ligne de niveau supérieur et d'appliquer les autorisations habituelles à certains groupes d'ordinateurs client de niveau inférieur. Pour que les autorisations habituelles s'appliquent, vous devez supprimer les autorisations hors ligne.

Pour supprimer des autorisations hors lignes

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Permissions**.

   Lorsque vous sélectionnez Permissions dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des autorisations. Le panneau de détails affiche aussi le statut actuel des autorisations hors lignes de chaque protocole dans la colonne Offline (hors ligne).

4. Dans le panneau de détails, cliquez droit sur le protocole pour lequel vous souhaitez supprimer les autorisations hors ligne, puis cliquez sur **Remove Offline**.

   Vous pouvez supprimer les autorisations hors ligne de plusieurs protocoles en même temps. Pour ce faire, procédez comme suit:

a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
b) Cliquez droit sur la sélection, puis cliquez sur **Remove Offline**.

Les autorisations adoptent alors le statut hors ligne «Use Regular» (utiliser habituel).

Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion des règles d'audit et de réplication hors ligne des protocoles

Pour une description détaillée de la fonction Auditing & Shadowing (audit et réplication) pour les protocoles, consultez le chapitre «Gestion des règles d'audit et de réplication des protocoles.»

Les règles d'audit et de réplication hors ligne peuvent avoir un des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les règles d'audit et de réplication ne sont pas définies pour le protocole. Il s'agit du statut par défaut.
Configured	Indique que les règles d'audit et de réplication sont définies pour le protocole.
No Audit	Indique une des situations suivantes: • Les droits d'audit ne sont pas définis pour tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du protocole. • Tous les utilisateurs et les groupes indiqués dans les règles d'audit et de réplication du protocole sont supprimés. • Le compte Everyone n'a ni droits d'audit ni droits de réplication et c'est le seul compte spécifié dans les règles d'audit et de réplication du protocole.
Use Regular	Indique que l'héritage des règles d'audit et de réplication hors ligne est bloqué et que les règles d'audit et de réplication habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des règles habituelles est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des règles habituelles permet d'empêcher l'application des autorisations hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur L'application des règles habituelles, consultez le chapitre intitulé «Suppression de règles d'audit et de réplication hors ligne.»

La gestion des règles d'audit et de réplication hors ligne comprend les tâches suivantes:

- Définition et édition de règles d'audit et de réplication hors ligne
- Révocation de règles d'audit et de réplication hors ligne
- Suppression de règles d'audit et de réplication hors ligne

Définition et édition de règles d'audit et de réplication hors ligne

Pour définir et éditer des règles d'audit et de réplication hors ligne

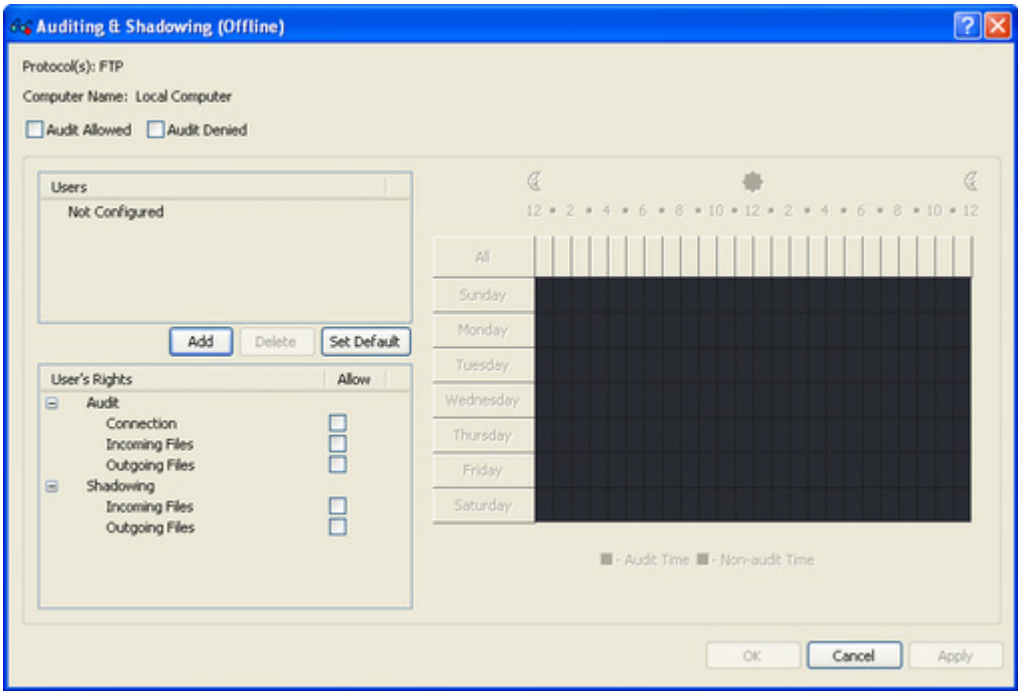
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors lignes pour chaque protocole dans la colonne Offline (hors ligne).
4. Dans le panneau de détails, procédez comme suit:
   - Cliquez droit sur le protocole pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur **Set Offline Auditing & Shadowing**.
     - OU -
   - Sélectionnez le protocole pour lequel vous souhaitez définir ou éditer des règles, puis cliquez sur le bouton **Set Offline Auditing & Shadowing** de la barre d'outils.

   La boîte de dialogue Auditing & Shadowing (Offline) apparaît.



5. Dans la boîte de dialogue **Auditing & Shadowing (Offline)**, procédez comme suit:

ACTION	PROCEDURE
Définir des règles d'audit et de réplication par défaut	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies d'accès à un protocole. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un protocole. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Set Default**. *Les règles d'audit et de réplication par défaut s'appliquent aux groupes Users et Everyone. Pour en savoir plus sur les droits d'audit et de réplication définis pour ces comptes par défaut, consultez le chapitre intitulé* «Gestion des règles d'audit et de réplication de protocoles.»
Définir des règles d'audit et de réplication pour un utilisateur ou un groupe supplémentaire	1. Dans la zone supérieure gauche de la boîte de dialogue, indiquez les événements à répertorier dans le journal d'audit. Cochez la case **Audit Allowed** pour consulter les tentatives réussies d'accès à un protocole. Cochez la case **Audit Denied** pour consulter les tentatives infructueuses d'accès à un protocole. 2. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, cliquez sur **Add**. *La boîte de dialogue Select Users or Groups apparaît*. 3. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez le nom de l'utilisateur ou du groupe, puis cliquez sur **OK**. *Les utilisateurs et les groupes que vous ajoutez s'affichent dans le champ Users du panneau supérieur gauche de la boîte de dialogue Auditing & Shadowing (Offline).* 4. Dans le champ **Users** du panneau supérieur gauche de la boîte

ACTION	PROCEDURE
	de dialogue **Auditing & Shadowing (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité. *Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL*. 5. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue **Auditing & Shadowing (Offline)**, cochez ou décochez la case **Allow** située en regard des droits appropriés. *Dans le panneau de droite de la boîte de dialogue Auditing & Shadowing (Offline), vous pouvez indiquer les jours et les horaires (par exemple, de 7h00 à 17h00 du lundi au vendredi) pendant lesquels les règles définies pour un utilisateur particulier s'appliquent ou non. Utilisez le bouton gauche de la souris et sélectionnez la période pendant laquelle la règle est appliquée (période d'audit). Utilisez le bouton droit de la souris et sélectionnez la période pendant laquelle la règle n'est pas appliquée (période de non audit)*.
Changer des règles d'audit et de réplication pour un utilisateur ou un groupe existant	1. Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité. 2. Dans le champ **User's Rights** du panneau inférieur gauche de la boîte de dialogue, cochez ou décochez la case **Allow** située en regard des droits d'accès appropriés.
Supprimer un utilisateur ou un groupe existant et les règles	• Dans le champ **Users** du panneau supérieur gauche de la boîte de dialogue, sélectionnez l'utilisateur ou le groupe souhaité, puis cliquez sur **Delete** ou appuyez sur la touche DELETE. *Quand vous supprimez un utilisateur ou un groupe, les règles associées à cet utilisateur ou groupe sont aussi supprimées*.

6. Cliquez sur **OK** ou sur **Apply**.

Révocation de règles d'audit et de réplication hors ligne

Vous pouvez redonner aux règles d'audit et de réplication hors ligne précédemment définies le statut non configuré. Si les règles hors ligne sont non définies, les règles habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des règles d'audit et de réplication hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors lignes pour chaque protocole dans la colonne Offline (hors ligne).
4. Dans le panneau de détails, cliquez droit sur le protocole pour lequel vous souhaitez révoquer les règles d'audit et de réplication hors ligne, puis cliquez sur **Undefine Offline**.

   Vous pouvez révoquer les règles d'audit et de réplication définies pour plusieurs protocoles à la fois. Pour ce faire, procédez comme suit:

   a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Undefine Offline**.

   Le statut hors ligne des règles d'audit et de réplication passe à «Not Configured» (non configuré).

Suppression de règles d'audit et de réplication hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage des règles d'audit et de réplication hors ligne de niveau supérieur et d'appliquer les règles d'audit et de réplication habituelles pour certains groupes d'ordinateurs client de niveau inférieur. Pour que les règles d'audit et de réplication habituelles s'appliquent, vous devez supprimer les règles d'audit et de réplication hors ligne.

Pour supprimer des règles d'audit et de réplication hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Auditing & Shadowing**.

   Lorsque vous sélectionnez Auditing & Shadowing dans l'arborescence, le panneau de détails affiche les protocoles pour lesquels vous pouvez définir des règles d'audit et de réplication. Le panneau de détails affiche aussi le statut actuel des règles hors lignes pour chaque protocole dans la colonne Offline (hors ligne).

4. Dans le panneau de détails, cliquez droit sur le protocole pour lequel vous souhaitez supprimer les règles d'audit et de réplication hors ligne, puis cliquez sur **Remove Offline**.

   Vous pouvez supprimer les règles d'audit et de réplication définies pour plusieurs protocoles à la fois. Pour ce faire, procédez comme suit:

   a) Dans le panneau de détails, sélectionnez plusieurs protocoles et cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.
   b) Cliquez droit sur la sélection, puis cliquez sur **Remove Offline**.

   Le statut hors ligne des règles d'audit et de réplication passe à «Use Regular» (utiliser habituelles).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion de la liste blanche de protocoles hors ligne

Pour obtenir une description détaillée de la fonction de liste blanche de protocoles, veuillez consulter le chapitre intitulé «Gestion de liste blanche de protocoles (Regular Profile).»

La liste blanche de protocoles hors ligne peut avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que la liste blanche n'est pas définie. Le message suivant s'affiche: «Offline Protocols White List is not configured.» (la liste blanche de protocoles hors ligne n'est pas configurée) Il s'agit du statut par défaut.
Configured	Indique que la liste blanche est définie.
Use Regular	Indique que l'héritage de la liste blanche hors ligne est bloqué et que la liste blanche habituelle s'applique. Le message suivant s'affiche: «Offline Protocols White List is configured to use Regular Protocols White List» (la liste blanche de protocoles hors ligne est configurée pour utiliser la liste blanche de protocoles habituelle). Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application de la liste blanche habituelle est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application de la liste blanche habituelle permet d'empêcher l'application de la liste blanche héritée d'un niveau supérieur à un groupe spécifique d'ordinateurs clients de niveau inférieur. Pour en savoir plus sur l'application de la liste blanche habituelle, consultez le chapitre intitulé «Suppression de liste blanche de protocoles hors ligne.»

La gestion de la liste blanche de protocoles hors ligne comprend les tâches suivantes:

- Définition de la liste blanche de protocoles hors ligne
- Édition de la liste blanche de protocoles hors ligne
- Copie des règles de la liste blanche de protocoles hors ligne
- Exportation et importation de la liste blanche de protocoles hors ligne

- Suppression des règles de la liste blanche de protocoles hors ligne
- Révocation de la liste blanche de protocoles hors ligne
- Suppression de liste blanche de protocoles hors ligne

Définition de la liste blanche de protocoles hors ligne

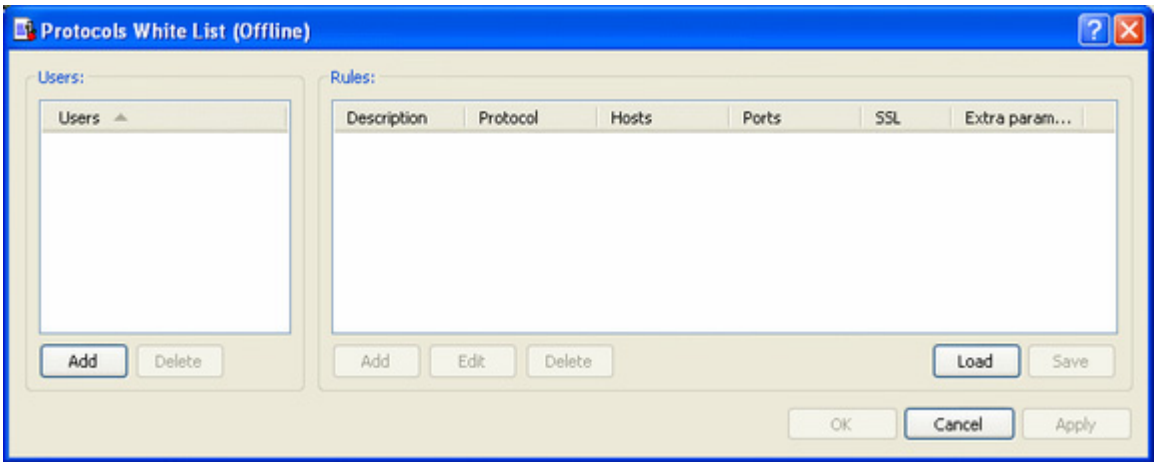
Pour définir la liste blanche de protocoles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Protocols White List (Offline) apparaît.



4. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la liste blanche de protocoles, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous ajoutez s'affichent dans le champ Users du panneau gauche de la boîte de dialogue Protocols White List (Offline).

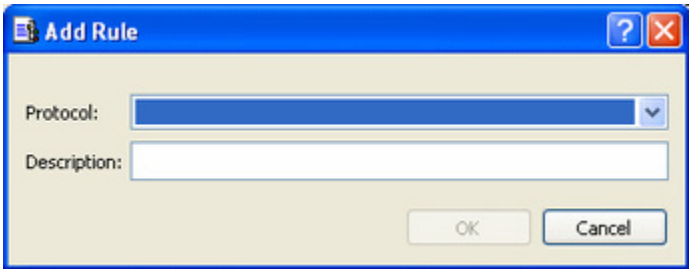
   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, puis cliquez sur **Delete**.

6. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez l'utilisateur ou le groupe souhaité.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Add Rule apparaît.



8. Dans la boîte de dialogue **Add Rule**, spécifiez les paramètres généraux et les paramètres propres au protocole pour cette règle. Pour spécifier les paramètres généraux, procédez comme suit:

   - Pour spécifier le protocole, dans le champ **Protocol:** cliquez sur le protocole de votre choix.
   - Pour spécifier le nom de la règle, saisissez un nom dans le champ **Description**.

   Pour spécifier les paramètres propres au protocole, procédez comme suit:

   - Pour spécifier les hôtes, dans le champ **Hosts:** saisissez les noms ou les adresses IP des hôtes, séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des hôtes, reportez-vous à la description du paramètre Hôtes.
   - Pour spécifier les ports, dans le champ **Ports:** saisissez les numéros de port séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des ports, reportez-vous à la description du paramètre Ports.
   - Pour configurer les options SSL, dans le champ **SSL**, cliquez sur l'une ou l'autre des options suivantes: **Allowed** (autorise les connexions SSL), **Denied** (n'autorise pas les connexions SSL), ou **Required** (toutes les connexions doivent utiliser SSL).
   - Pour spécifier l'ID(s) de l'expéditeur local MI, dans le champ **Local sender ID(s):** saisissez les identifiants d'utilisateur, séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des identifiants

de l'utilisateur, reportez-vous à la description du paramètre ID(s) d'expéditeur local.

- Pour spécifier le ou les ID(s) de destinataire distant MI, dans le champ **Remote recipient ID(s):** saisissez les identifiants d'utilisateur séparés par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des identifiants d'utilisateur, reportez-vous à la description du paramètre ID(s) de destinataire distant.
- Pour spécifier les expéditeurs d'emails, dans le champ **Local sender Email(s):** saisissez les adresses d'expéditeur séparées par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des adresses de l'expéditeur, reportez-vous à la description du paramètre Email(s) d'expéditeur local.
- Pour spécifier les destinataires d'emails, dans le champ **Remote recipient Email(s):** saisissez les adresses de destinataire séparées par des virgules ou des points-virgules. Pour en savoir plus sur le mode de définition des adresses de destinataire, reportez-vous à la description du paramètre Email(s) de destinataire distant.
- Pour spécifier les sites de réseaux sociaux, cochez ou décochez les cases appropriées dans le champ **Social Networks:** Pour en savoir plus, reportez-vous à la description du paramètre Réseaux sociaux.
- Pour spécifier les services de messagerie Web, cochez ou décochez les cases appropriées dans le champ **Web Mail Services:** Pour en savoir plus, reportez-vous à la description du paramètre Services de messagerie.

9. Cliquez sur **OK**.

   La règle ainsi créée figure dans le champ Rules du panneau droit de la boîte de dialogue Protocols White List (Offline).

10. Cliquez sur **OK** ou sur **Apply**.

    Les utilisateurs ou les groupes auxquels s'applique la règle de la liste blanche sont affichés dans le champ White List de l'arborescence de console.

    Si vous sélectionnez un utilisateur ou un groupe auquel la règle de la liste blanche s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

    - **Protocol** La règle applicable au protocole.
    - **Description** Le nom de la règle.
    - **Hosts** Indique les hôtes autorisés pour cette règle.
    - **Ports** Indique les ports autorisés pour cette règle.
    - **SSL** Indique l'option SSL sélectionnée. Valeurs possibles: **Allowed** (autorise les connexions SSL), **Denied** (n'autorise pas les connexions SSL), et **Required** (toutes les connexions doivent utiliser SSL).
    - **Extra parameters** Indique les paramètres supplémentaires propres au protocole pour cette règle. Ces paramètres incluent: **From** (indique les identifiants de l'expéditeur pour la messagerie instantanée et les adresses email de l'expéditeur pour la messagerie Web) et **To** (indique les identifiants du destinataire pour la messagerie instantanée et les adresses email du destinataire pour la messagerie Web).
    - **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs clients qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs clients qui travaillent hors ligne.

Vous pouvez définir des listes blanches de protocoles différentes selon qu'elles s'appliquent en ligne ou hors ligne pour le même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur le mode de définition de la liste blanche de protocoles en ligne, reportez-vous au chapitre intitulé «Gestion de la liste blanche des protocoles.»

Édition de liste blanche de protocoles hors ligne

Vous pouvez modifier les valeurs des paramètres spécifiées pour une règle de liste blanche hors ligne à tout instant.

Pour modifier une règle de liste blanche hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquer droit sur **White List**, cliquer sur **Manage Offline**, puis faire la chose suivante:
   a) Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans l'option Rules du panneau droit de la boîte de dialogue.
   b) Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.
   - OU -
   Cliquez droit sur la règle, puis cliquez sur **Edit**.

   - OU -

   Dans **Protocols**, développez **White List**, puis procédez comme suit:
   a) Dans **White List**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans le panneau de détails.
   b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.

- OU -

Dans le panneau de détails, double-cliquez sur la règle que vous souhaitez modifier.

La boîte de dialogue Edit Rule apparaît.

4. Dans la boîte de dialogue **Edit Rule**, modifiez les paramètres des règles en fonction de vos besoins.
5. Cliques sur **OK** pour valider les modifications.

Copie des règles de la liste blanche de protocoles hors ligne

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles existantes de la liste blanche de protocoles hors ligne.

Pour copier une règle de liste blanche hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **White List**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Protocols White List (Offline) apparaît.
4. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle que vous souhaitez copier.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles de liste blanche auxquelles ils sont soumis dans l'option Rules du panneau droit de la boîte de dialogue.
5. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, cliquez droit sur la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

   La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Lorsque vous utilisez la combinaison de touches CTRL+X pour couper la règle, la règle ne sera coupée qu'une fois copiée.

6. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

7. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes auxquels s'applique la règle que vous souhaitez copier, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous ajoutez s'affichent dans le champ Users du panneau gauche de la boîte de dialogue Protocols White List (Offline).

8. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez appliquer la règle ainsi copiée.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

9. Dans le panneau droit de la boîte de dialogue **Protocols White List (Offline)**, cliquez droit sur le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée figure dans le champ Rules du panneau droit de la boîte de dialogue Protocols White List (Offline).

10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de la liste blanche de protocoles hors ligne

Vous pouvez exporter toutes vos règles de la liste blanche de protocoles hors ligne en cours dans un fichier .pwl puis importer et utiliser celui-ci sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter la liste blanche de protocoles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Cliquez droit sur **White List**, puis cliquez sur **Save Offline.**

- OU -

- Sélectionnez **White List**, puis cliquez sur l'option **Save Offline** de la barre d'outils.

  - OU -

- Développez **White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Save Offline**.

  - OU -

- Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur la règle de liste blanche, puis cliquez sur **Save**.

  - OU –

- Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur l'option **Save Offline** de la barre d'outils.

  - OU -

- Cliquez droit sur **White List**, puis cliquez sur **Manage Offline**. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, cliquez sur **Save**.

La boîte de dialogue Save As apparaît.

4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .pwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez la liste blanche de protocoles hors ligne, celle-ci est sauvegardée dans un fichier doté d'une extension .pwl.

Pour importer la liste blanche de protocoles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:

   - Cliquez droit sur **White List**, puis cliquez sur **Load Offline**.

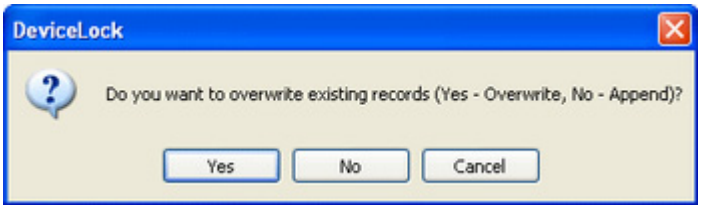
     - OU -

- Sélectionnez **White List**, puis cliquez sur l'option **Load Offline** de la barre d'outils.
  - OU -
- Développez **White List**, cliquez droit sur l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur **Load Offline**.
  - OU -
- Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche. Dans le panneau de détails, cliquez droit sur la règle de liste blanche, puis cliquez sur **Load**.
  - OU -
- Développez **White List**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes indiqués dans la liste blanche, puis cliquez sur l'option **Load Offline** de la barre d'outils.
  - OU -
- Cliquez droit sur **White List**, puis cliquez sur **Manage Offline**. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, cliquez sur **Load**.

La boîte de dialogue Open apparaît.

4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Si la liste blanche de protocoles hors ligne est déjà définie et que vous choisissez d'importer une nouvelle liste blanche hors ligne, le champ de message suivant s'affiche.



   Dans le champ de message, cliquez sur **Yes** pour écraser la liste blanche hors ligne existante. Cliquez sur **No** pour ajouter une nouvelle liste blanche hors ligne à la liste blanche hors ligne existante.

Suppression de règles de liste blanche de protocoles hors ligne

Vous pouvez supprimer les règles de liste blanche hors ligne individuelles qui ne sont plus nécessaires.

Pour supprimer une règle de liste blanche hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

a) Ouvrez DeviceLock Service Settings Editor.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:

- Développez **White List**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.
  Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.
  - OU -
- Développez **White List**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.
  - OU -
- Cliquez droit sur **White List**, puis cliquez sur **Manage Offline**. Dans le champ **Users** du panneau gauche de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le champ **Rules** du panneau droit de la boîte de dialogue **Protocols White List (Offline)**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.

Révocation de liste blanche de protocoles hors ligne

Vous pouvez redonner à la liste blanche hors ligne précédemment définie le statut non configurée. Si la liste blanche hors ligne est indéfinie, la liste blanche habituelle s'applique aux ordinateurs client hors ligne.

Pour révoquer la liste blanche de protocoles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

a) Ouvrez DeviceLock Service Settings Editor.
b) Dans l'arborescence, développez **DeviceLock Service**.

Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

a) Ouvrez Group Policy Object Editor.
b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **White List** puis cliquez sur **Undefine Offline**.

Le statut hors ligne de la liste blanche passe à «Not Configured» (non configuré).

Lorsque vous sélectionnez White List dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Protocols White List is not configured.» (la liste blanche de protocoles hors ligne n'est pas configurée)

Suppression de liste blanche de protocoles hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer l'héritage de la liste blanche hors ligne de niveau supérieur et d'appliquer la liste blanche habituelle à certains groupes d'ordinateurs client de niveau inférieur. Pour que la liste blanche de protocoles habituelle s'applique, vous devez supprimer la liste blanche de protocoles hors ligne.

Pour supprimer la liste blanche de protocoles hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez DeviceLock Service.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **White List** puis cliquez sur **Remove Offline**.

   Le statut hors ligne de la liste blanche passe à «Use Regular» (utiliser habituel).

   Lorsque vous sélectionnez White List dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Protocols White List is configured to use Regular Protocols White List» (la liste blanche de protocoles hors ligne est configurée pour utiliser la liste blanche de protocoles habituelle).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans DeviceLock Management Console.

Gestion des règles contextuelles pour les protocoles hors ligne

Pour une description détaillée de la fonction Content-Aware Rules (règles contextuelles) pour les protocoles, consultez le chapitre «Règles contextuelles pour les protocoles (Regular Profile).»

Les règles contextuelles hors ligne peuvent avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les règles contextuelles ne sont pas définies. Le message suivant s'affiche: «Offline Content-Aware Rules are not configured» (Les règles contextuelles hors ligne ne sont pas configurées). Il s'agit du statut par défaut.

STATUT	DESCRIPTION
Configured	Indique que les règles contextuelles sont définies.
Use Regular	Indique que l'héritage des règles contextuelles hors ligne est bloqué et que les règles contextuelles habituelles s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager. L'application des règles contextuelles habituelles est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des règles contextuelles habituelles permet d'empêcher l'application des règles contextuelles hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des règles contextuelles habituelles, consultez le chapitre intitulé «Suppression de règles contextuelles hors ligne.»

La gestion des règles contextuelles hors ligne comprend les tâches suivantes:

- Définition de règles contextuelles hors ligne
- Modification de règles contextuelles hors ligne
- Copie de règles contextuelles hors ligne
- Exportation et importation de règles contextuelles hors ligne
- Suppression de règles contextuelles hors ligne
- Révocation de règles contextuelles hors ligne
- Suppression de règles contextuelles hors ligne

Définition de règles contextuelles hors ligne

Les règles contextuelles sont créées sur la base des groupes de contenus intégrés ou sur la base des groupes de contenus personnalisés. Pour plus d'informations sur ces groupes, voir «Configuration des paramètres de détection de contenu.»

Pour définir une règle contextuelle hors ligne

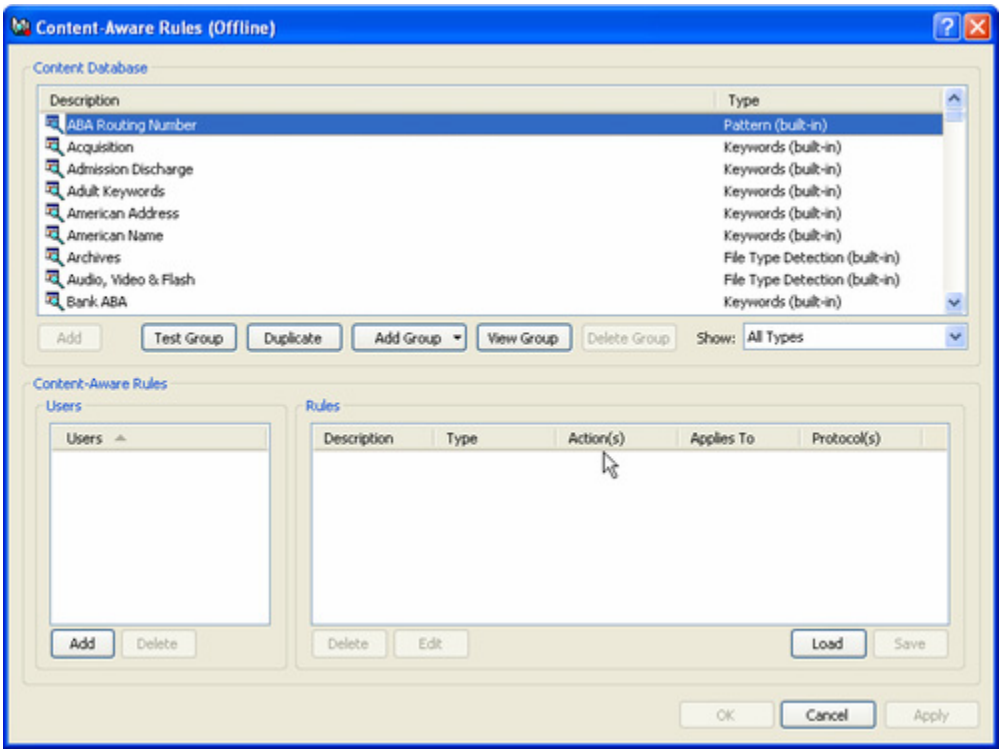
1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.

3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules (Offline) apparaît.



4. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

5. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez les noms des utilisateurs ou des groupes pour lesquels vous souhaitez définir la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes ajoutés s'affichent dans le champ Users du panneau inférieur gauche de la boîte de dialogue Content-Aware Rules (Offline).

   Pour supprimer un utilisateur ou un groupe, sélectionnez l'utilisateur ou le groupe dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, puis cliquez sur **Delete** ou appuyez sur la touche DELETE.

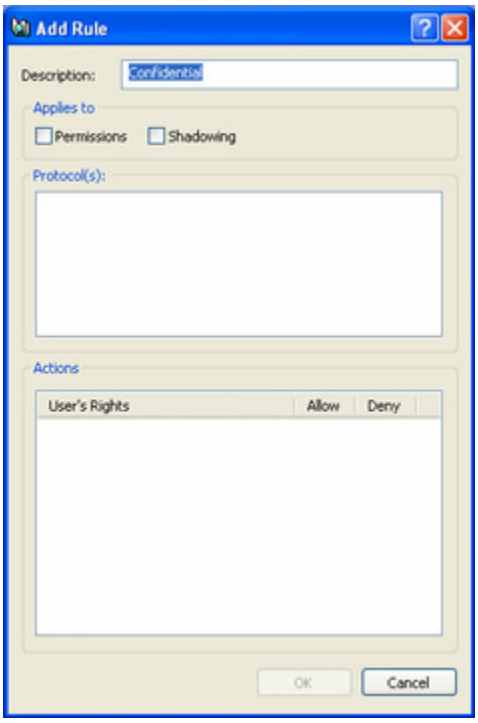
6. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez les utilisateurs ou les groupes pour lesquels vous souhaitez définir la règle.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

7. Dans le champ **Content Database** du panneau supérieur de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez le groupe de contenus souhaité, puis cliquez sur **Add**.

   Remarque: Vous ne pouvez indiquer qu'un seul groupe de contenus par règle contextuelle.

   La boîte de dialogue Add Rule apparaît.



8. Dans le champ **Description** de la boîte de dialogue **Add Rule**, saisissez le nom de la règle contextuelle.

   Par défaut, la règle contextuelle a le même nom que le groupe de contenus indiqué mais vous pouvez saisir un nom différent.

9. Dans **Applies to**, indiquez le type d'opération associé à la règle. Les options disponibles sont les suivantes:

   - **Permissions**: Indique que la règle s'appliquera aux opérations de contrôle d'accès.
   - **Shadowing**: Indique que la règle s'appliquera aux opérations de copie de réplication.
   - **Permissions, Shadowing**: Indique que la règle s'appliquera aux opérations de contrôle d'accès et de copie de réplication.

10. Dans **Protocol(s)**, sélectionnez le ou les types de protocoles auxquels vous souhaitez que cette règle s'applique.

    Les règles contextuelles peuvent s'appliquer aux protocoles suivants: FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, Réseaux sociaux, messagerie Web, Windows Messenger, et Yahoo Messenger.

Si plusieurs protocoles sont sélectionnés dans le paramètre Action(s), la boîte de dialogue affichera uniquement les droits d'accès qui sont communs à tous les protocoles sélectionnés.

11. Dans le champ **Action(s)**, indiquez les actions utilisateur qui sont autorisées ou non sur les protocoles, et celles qui sont consignées dans le journal de réplication.

    Pour en savoir plus sur les droits d'utilisateur susceptibles de figurer dans les règles contextuelles, consultez les chapitres intitulés «Règles contextuelles pour opérations de contrôle d'accès» et «Règles contextuelles pour opérations de copie de réplication.»

12. Cliquez sur **OK**.

    La règle ainsi créée s'affiche dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules (Offline).

13. Cliquez sur **OK** ou **Apply** pour appliquer la règle.

    Les utilisateurs ou les groupes auxquels s'applique la règle contextuelle figurent dans la section Content-Aware Rules de l'arborescence. Si vous sélectionnez un utilisateur ou un groupe auquel la règle contextuelle s'applique dans l'arborescence, le panneau de détails affiche des informations détaillées sur la règle en question. Ces informations concernent notamment:

    - **Description** Le nom de la règle. Par défaut, la règle a le même nom que le groupe de contenus indiqué.
    - **Type** Le type de l'analyse de contenus. Valeurs possibles: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties**, et **Complex**. **File Type Detection** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs signatures propres. **Keywords** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des mots clés et des expressions spécifiés. **Pattern** indique que la connaissance et l'identification des données et des fichiers s'effectuent en fonction des modèles de textes décrits par les expressions régulières Perl. **Document Properties** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction de leurs propriétés. **Complex** indique que la reconnaissance et l'identification des fichiers s'effectuent en fonction du contenu décrit par une expression booléenne.
    - **Action(s)** affiche les actions utilisateur qui sont autorisées ou non sur les protocoles, et celles qui sont consignées dans le journal de réplication.
    - **Applies To** Valeurs possibles: **Permissions**, **Shadowing**, et **Permissions, Shadowing**. **Permissions** indique que la règle s'applique aux contrôles d'accès. **Shadowing** indique que la règle s'applique aux copies de réplication. **Permissions, Shadowing** indique que la règle s'applique à la fois aux contrôles d'accès et aux copie de réplication.
    - **Protocol(s)** Les protocoles auxquels s'applique la règle.
    - **Profile** Valeurs possibles: **Regular** et **Offline**. **Regular** indique que la règle s'applique aux ordinateurs client qui travaillent en ligne. **Offline** indique que la règle s'applique aux ordinateurs client qui travaillent hors ligne.

      Vous pouvez définir des règles contextuelles différentes selon qu'elles s'appliquent en ligne ou hors ligne au même utilisateur ou groupe d'utilisateurs. Pour en savoir plus sur la façon de définir les règles contextuelles pour les protocoles en ligne, consultez le chapitre intitulé «Gestion des règles contextuelles.»

Modification de règles contextuelles hors ligne

Vous pouvez modifier les propriétés des règles contextuelles, notamment les propriétés Description, Applies To, Protocol(s), Actions.

Pour modifier une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **Content-Aware Rules**, cliquez sur **Manage Offline**, puis procédez comme suit:
   a) Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
   b) Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, sous **Rules**, sélectionnez la règle que vous souhaitez modifier, puis cliquez sur **Edit**.

   - OU -

   Dans **Protocols**, développez **Content-Aware Rules**, puis procédez comme suit:
   a) Dans **Content-Aware Rules**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier la règle.
   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans le panneau de détails.
   b) Dans le panneau de détails, cliquez droit sur la règle à modifier, puis cliquez sur **Edit**.
   - OU -
   Dans le panneau de détails, double-cliquez sur la règle à modifier.

   La boîte de dialogue Edit Rule apparaît.
4. Dans la boîte de dialogue **Edit Rule**, modifiez les propriétés de règles en fonction de vos besoins.

5. Cliques sur **OK** pour valider les modifications.

Copie de règles contextuelles hors ligne

Vous pouvez effectuer un couper/coller, un copier/coller ou un glisser/déposer pour réutiliser des règles contextuelles hors ligne existantes.

Pour copier une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Manage Offline** de la barre d'outils.

   La boîte de dialogue Content-Aware Rules (Offline) apparaît.
4. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sous **Users**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez copier la règle.

   Lorsque vous sélectionnez des utilisateurs ou des groupes, vous pouvez afficher les règles contextuelles qui s'appliquent à eux dans l'option Rules du panneau inférieur droit de la boîte de dialogue.
5. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, sous **Rules**, sélectionnez la règle que vous souhaitez copier, puis cliquez sur **Copy** ou **Cut**.

   La règle que vous coupez ou copiez est automatiquement copiée dans le presse-papiers.

   Vous pouvez utiliser les combinaisons de touches CTRL+C, CTRL+X et CTRL+V pour copier, couper et coller la règle. Si vous utilisez la combinaison de touches CTRL+X pour couper la règle, cette règle ne sera coupée qu'une fois collée.

   Pour effectuer un glisser/déposer, sélectionnez la règle et déplacez-la sur l'utilisateur ou le groupe d'utilisateurs auxquels vous désirez appliquer la règle ainsi copiée.

6. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sous **Users**, cliquez sur **Add**.

   La boîte de dialogue Select Users or Groups apparaît.

7. Dans la boîte de dialogue **Select Users or Groups**, champ **Enter the object names to select**, saisissez les noms des utilisateurs ou des groupes dont vous souhaitez copier la règle, puis cliquez sur **OK**.

   Les utilisateurs et les groupes que vous avez ajoutés s'affichent sous Users dans le panneau inférieur gauche de la boîte de dialogue Content-Aware Rules (Offline).

8. Dans le panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sous Users, sélectionnez les utilisateurs ou les groupes dont vous souhaitez copier la règle.

   Pour sélectionner plusieurs utilisateurs ou groupes d'utilisateurs, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

9. Dans le panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez droit dans le panneau **Rules** puis cliquez sur **Paste**.

   La règle ainsi copiée est affichée dans le champ Rules du panneau inférieur droit de la boîte de dialogue Content-Aware Rules (Offline).

10. Cliquez sur **OK** ou **Apply** pour appliquer la règle copiée.

Exportation et importation de règles contextuelles hors ligne

Vous pouvez exporter toutes vos règles contextuelles en cours dans un fichier .cwl susceptible d'être importé et utilisé sur un autre ordinateur. L'exportation et l'importation peuvent aussi servir à la sauvegarde.

Pour exporter des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Save Offline**.
     - OU -
   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Save Offline** de la barre d'outils.

- OU -

- Développez **Content-Aware Rules**, cliquez droit sur n'importe quel utilisateur ou groupe, puis cliquez sur **Save Offline**.

  - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Save**.

  - OU -

- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Save Offline** de la barre d'outils.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage (Offline)**. Dans le champ **Users** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Save**.

La boîte de dialogue Save As apparaît.

4. Dans le champ **Save in** de la boîte de dialogue **Save As**, sélectionnez l'emplacement où vous souhaitez sauvegarder le fichier .cwl.
5. Dans le champ **File name**, saisissez le nom de fichier souhaité.
6. Cliquez sur **Save**.

   Lorsque vous exportez des règles, celles-ci sont sauvegardées dans un fichier à extension .cwl.

Pour importer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:

   - Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Load Offline**.

     - OU -

   - Sélectionnez **Content-Aware Rules**, puis cliquez sur l'option **Load Offline** de la barre d'outils.

     - OU -

- Développez **Content-Aware Rules**, cliquez droit sur n'importe quel utilisateur ou groupe, puis cliquez sur **Load Offline**.

  - OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle, puis cliquez sur **Load**.

  - OU -

- Développez **Content-Aware Rules**, sélectionnez l'un ou l'autre des utilisateurs ou des groupes auxquels la règle s'applique, puis cliquez sur l'option **Load Offline** de la barre d'outils.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**. Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, cliquez sur **Load**.

La boîte de dialogue Open apparaît.

4. Dans la liste **Look in** de la boîte de dialogue **Open**, cliquez sur l'emplacement qui contient le fichier que vous souhaitez importer.
5. Dans la liste des dossiers, identifiez et ouvrez le dossier qui contient le fichier.
6. Cliquez sur le fichier, puis sur **Open**.

   Vous ne pouvez importer qu'un seul fichier .cwl à la fois.

Suppression de règles contextuelles hors ligne

Vous pouvez supprimer les règles contextuelles hors ligne individuelles qui ne sont plus nécessaires.

Pour supprimer une règle contextuelle hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, effectuez l'une ou l'autre des actions suivantes:
   - Développez **Content-Aware Rules**, cliquez droit sur l'utilisateur ou le groupe auquel la règle s'applique, puis cliquez sur **Delete user**.

Si vous supprimez un utilisateur ou un groupe, la règle associée à cet utilisateur ou à ce groupe est automatiquement supprimée.

- OU -

- Développez **Content-Aware Rules**, puis sélectionnez l'utilisateur ou le groupe auquel la règle s'applique. Dans le panneau de détails, cliquez droit sur la règle associée à l'utilisateur ou au groupe en question, puis cliquez sur **Delete**.

  - OU -

- Cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage Offline**. Dans le champ **Users** du panneau inférieur gauche de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez l'utilisateur ou le groupe auquel s'applique la règle. Dans le champ **Rules** du panneau inférieur droit de la boîte de dialogue **Content-Aware Rules (Offline)**, sélectionnez la règle puis cliquez sur **Delete** ou cliquez droit sur la règle et cliquez sur **Delete**.

  Pour sélectionner plusieurs règles à supprimer, cliquez dessus tout en maintenant enfoncée la touche MAJ ou la touche CTRL.

Révocation de règles contextuelles hors ligne

Vous pouvez redonner aux règles contextuelles hors ligne précédemment définies le statut non configuré. Si les règles hors ligne sont non définies, les règles habituelles s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:

   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:

   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:

   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.

2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Undefine Offline**.

   Les règles contextuelles adopte alors le statut hors ligne «Not Configured» (non configuré).

   Lorsque vous sélectionnez **Content-Aware Rules** dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Content-Aware Rules are not configured» (Les règles contextuelles hors ligne ne sont pas configurées).

Suppression de règles contextuelles hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer les règles contextuelles hors ligne héritées d'un niveau supérieur et d'appliquer les règles contextuelles habituelles à certains groupes d'ordinateurs client de niveau inférieur. Pour que les règles contextuelles habituelles s'appliquent, vous devez supprimer les règles contextuelles hors ligne.

Pour supprimer des règles contextuelles hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Remove Offline**.

   Les règles contextuelles adoptent alors le statut hors ligne «Use Regular» (utiliser habituelles).

   Lorsque vous sélectionnez **Content-Aware Rules** dans l'arborescence, le message suivant apparaît dans le panneau de détails: «Offline Content-Aware Rules are configured to use Regular Content-Aware Rules» (Les règles contextuelles hors ligne sont configurées pour utiliser les règles contextuelles habituelles).

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Gestion des paramètres de sécurité des protocoles hors ligne

Pour une description détaillée de la fonction Security Settings (paramètres de sécurité) pour les protocoles, consultez le chapitre «Gestion des paramètres de sécurité des protocoles.»

Les paramètres de sécurité hors ligne peuvent avoir l'un ou l'autre des statuts suivants:

STATUT	DESCRIPTION
Not Configured	Indique que les paramètres de sécurité ne sont pas définis pour les protocoles. Il s'agit du statut par défaut.
Enabled	Indique que les paramètres de sécurité sont activés pour les protocoles.
Disabled	Indique que les paramètres de sécurité sont désactivés pour les protocoles.
Use Regular	Indique que l'héritage des paramètres de sécurité hors ligne est bloqué et que les paramètres de sécurité habituels s'appliquent. Les paramètres Offline DeviceLock ne peuvent avoir ce statut que dans DeviceLock Service Settings Editor ou DeviceLock Groupe Policy Manager.

STATUT	DESCRIPTION
	L'application des paramètres de sécurité habituels est utile si vous utilisez des fichiers Group Policy ou DeviceLock Service Settings (.dls) pour étendre les politiques DeviceLock à l'ensemble de votre réseau. L'application des paramètres de sécurité habituels permet d'empêcher l'application des paramètres de sécurité hors ligne héritées d'un niveau supérieur à un groupe spécifique d'ordinateurs client de niveau inférieur. Pour en savoir plus sur l'application des paramètres de sécurité habituels, consultez le chapitre intitulé «Suppression de paramètres de sécurité hors ligne.»

La gestion des paramètres de sécurité hors ligne comprend les tâches suivantes:

- Définition et modification de paramètres de sécurité hors ligne
- Révocation de paramètres de sécurité hors ligne
- Suppression de paramètres de sécurité hors ligne

Définition et modification de paramètres de sécurité hors ligne

Pour définir et modifier les paramètres de sécurité hors ligne

1. Si vous utilisez DeviceLock Management Console, procédez comme suit:
   a) Ouvrez DeviceLock Management Console et connectez-le à l'ordinateur qui exécute DeviceLock Service.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Sélectionnez **Security Settings**. Dans le panneau de détails, cliquez droit sur le paramètre de sécurité, puis cliquez sur **Enable Offline** ou **Disable Offline**.
     Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
     - OU -
   - Cliquez droit sur **Security Settings**, puis cliquez sur **Manage Offline**. Dans la boîte de dialogue **Security Settings (Offline)** qui s'ouvre, cochez ou décochez la case appropriée, puis cliquez sur **OK**.

Pour ouvrir la boîte de dialogue Security Settings (Offline), vous pouvez aussi sélectionner Security Settings, puis cliquer sur l'option Manage Offline de la boîte d'outils.

Remarque: Toutes les case de la boîte de dialogue **Security Settings (Offline)** ont trois statuts: coché, décoché et indéterminé qui correspondent aux statuts Enabled (activé), Disabled (désactivé) et Not Configured (non configuré) des paramètres de sécurité.

Le paramètre de sécurité passe du statut hors ligne «Not Configured» au statut hors ligne «Enabled» ou «Disabled».

Révocation de paramètres de sécurité hors ligne

Vous pouvez redonner aux paramètres de sécurité hors ligne précédemment définis le statut non configuré. Si les paramètres de sécurité hors ligne sont non définis, les paramètres de sécurité habituels s'appliquent aux ordinateurs client hors ligne.

Pour révoquer des paramètres de sécurité hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, cliquez droit sur **DeviceLock Settings** ou **DeviceLock Servic**e, puis cliquez sur **Load Service Settings** pour ouvrir le fichier XML à l'aide de stratégies DeviceLock prédéfinies.
   c) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, procédez comme suit:
   - Sélectionnez **Security Settings**. Dans le panneau de détails, cliquez droit sur le paramètre de sécurité, puis cliquez sur **Undefine Offline**.
     Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
     - OU -
   - Cliquez droit sur **Security Settings**, puis cliquez sur **Manage Offline**. Dans la boîte de dialogue **Security Settings (Offline)** qui s'ouvre, remettez les cases appropriées en mode indéterminé, puis cliquez sur **OK**.
     Pour ouvrir la boîte de dialogue Security Settings (Offline), vous pouvez aussi sélectionner Security Settings, puis cliquer sur l'option Manage Offline de la boîte d'outils.

Remarque: Toutes les case de la boîte de dialogue **Security Settings (Offline)** ont trois statuts: coché, décoché et indéterminé qui correspondent aux statuts Enabled (activé), Disabled (désactivé) et Not Configured (non configuré) des paramètres de sécurité.

Le paramètre de sécurité adopte alors le statut hors ligne «Not Configured» (non configuré).

Suppression de paramètres de sécurité hors ligne

Si vous déployez des politiques DeviceLock à l'aide de fichiers Group Policy ou DeviceLock Service Settings (.dls), DeviceLock permet de bloquer les paramètres de sécurité hors ligne hérités d'un niveau supérieur et d'appliquer les paramètres de sécurité habituels à certains groupes d'ordinateurs client de niveau inférieur. Pour que les paramètres de sécurité habituels s'appliquent, vous devez supprimer les paramètres de sécurité hors ligne.

Pour supprimer des paramètres de sécurité hors ligne

1. Si vous utilisez DeviceLock Service Settings Editor, procédez comme suit:
   a) Ouvrez DeviceLock Service Settings Editor.
   b) Dans l'arborescence, développez **DeviceLock Service**.

   Si vous utilisez DeviceLock Group Policy Manager, procédez comme suit:
   a) Ouvrez Group Policy Object Editor.
   b) Dans l'arborescence, développez **Computer Configuration**, puis **DeviceLock**.
2. Développez **Protocols**.
3. Dans **Protocols**, sélectionnez **Security Settings**.

   Lorsque vous sélectionnez les paramètres de sécurité dans l'arborescence, ceux-ci s'affichent dans le panneau de détails.
4. Dans le panneau de détails, cliquez droit sur n'importe quel paramètre de sécurité à supprimer, puis cliquez sur **Remove Offline**.

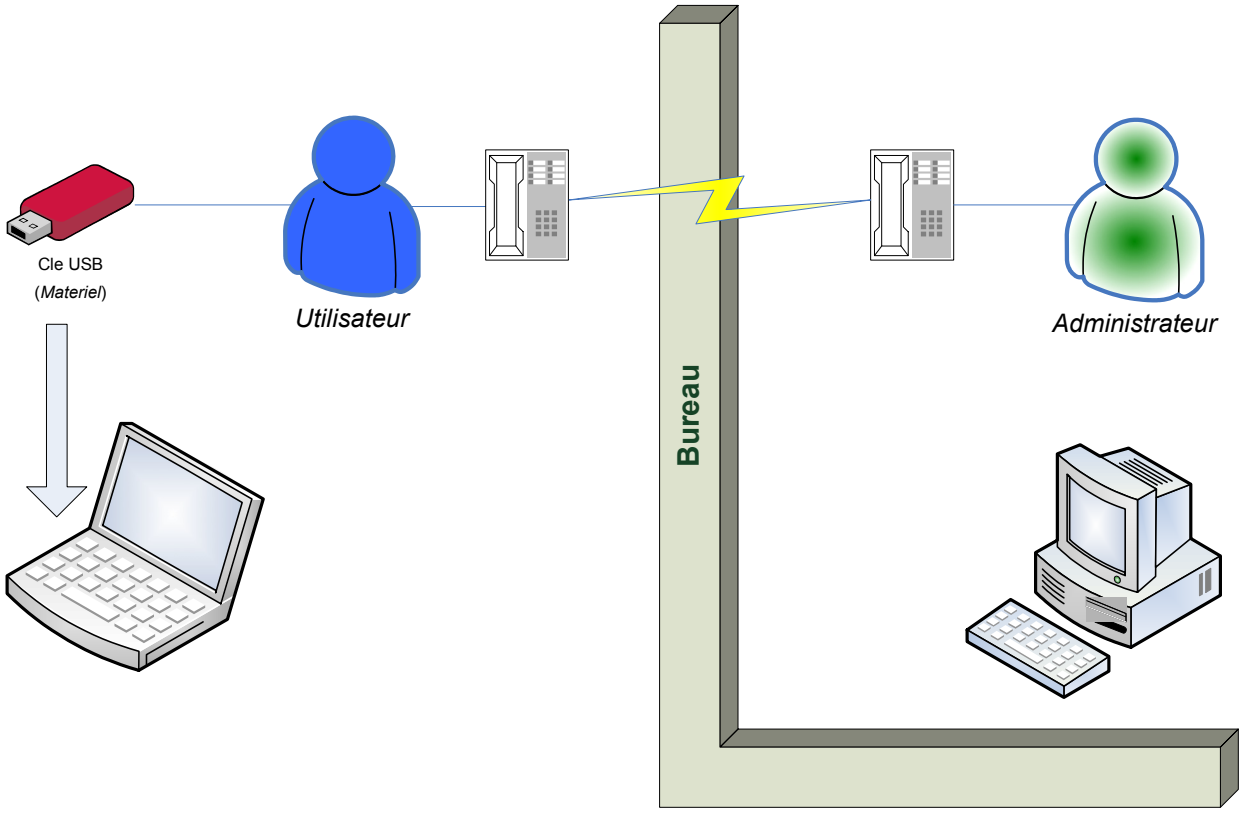
   Le paramètre de sécurité adopte alors le statut hors ligne «Use Regular».

   Le statut «Use Regular» des paramètres DeviceLock s'affiche en mode «Not Configured» (non configuré) dans la DeviceLock Management Console.

Temporary white list

Présentation

La fonction Temporary white list de DeviceLock permet d'attribuer des droits d'accès temporaires aux périphériques USB en l'absence de connexion au réseau. Les administrateurs fournissent téléphoniquement aux utilisateurs des codes d'accès spéciaux qui débloquent temporairement les périphériques requis.



Une temporary white list fonctionne comme une Device White List, à cela près qu'une connexion au réseau n'est pas nécessaire pour ajouter des périphériques et pour attribuer des droits d'accès à ceux-ci.

Remarque: Une liste blanche temporaire permet d'attribuer des droits d'accès à des périphériques USB bloqués aux deux niveaux: celui du port USB et au niveau typologique. Si certains périphériques figurant dans la liste blanche (p.ex. le lecteur flash USB) appartiennent aux deux niveaux: USB et typologique (amovible), les autorisations (le cas échéant) au niveau typologique sont ignorées comme au niveau du port USB.

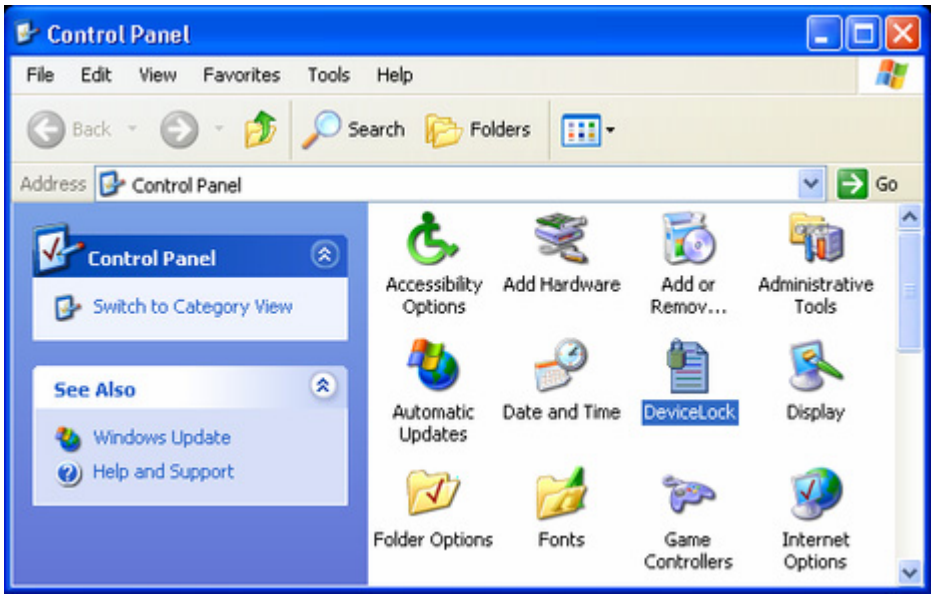
Pour créer et activer une temporary white list, contentez-vous de suivre les instructions détaillées suivantes:

1. L'administrateur génère un certificat cryptographique (DeviceLock Certificate) à l'aide de l'applet Certificate Generation Tool. Un DeviceLock Certificate est constitué de deux clés: une clé privée et une clé publique.
2. L'administrateur installe le DeviceLock Certificate (la clé publique) sur l'ordinateur d'un utilisateur. Cela active la temporary white list sur l'ordinateur de l'utilisateur.
3. Lorsqu'un utilisateur doit accéder à un périphérique USB, il exécute l'applet Temporary White List Authorization Tool du **Panneau de configuration** de Windows. Puis, l'utilisateur sélectionne le périphérique considéré dans une liste et un code alphanumérique (le **Device Code**) est généré. L'utilisateur peut alors fournir ce code par voie téléphoniquuuex ou via une session de chat Internet à l'administrateur de DeviceLock.
4. L'administrateur exécute alors le DeviceLock Signing Tool, charge le DeviceLock Certificate correspondant (la clé privée), saisit le **Device Code**, choisit une période d'accès temporaire appropriée (5, 15, etc. minutes ou jusqu'au débranchement du périphérique ou à la déconnexion de l'utilisateur), génère un **Unlock Code**, et transmet celui-ci à l'utilisateur.
5. A réception de l'**Unlock Code**, l'utilisateur le saisit dans le Temporary White List Authorization Tool. L'accès au périphérique considéré est alors accordé pour la période indiquée.

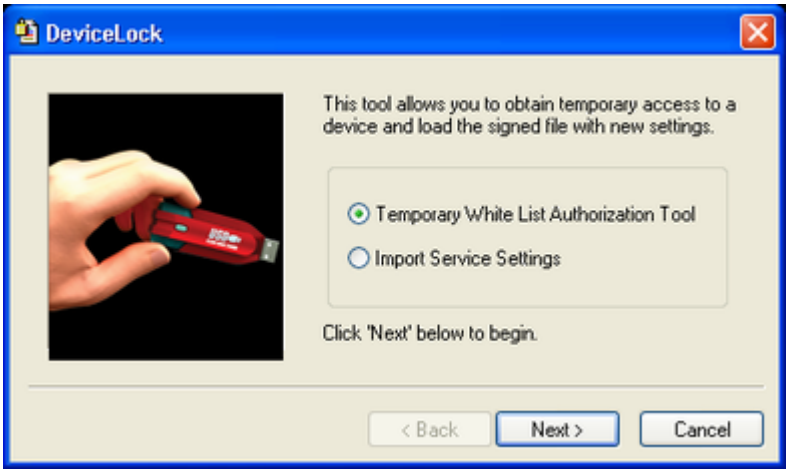
Temporary White List Authorization Tool

L'outil d'autorisation de temporary white list est l'applet du **Panneau de configuration** de Windows que les utilisateurs doivent utiliser pour bénéficier d'un accès temporaire aux périphériques.

Pour exécuter l'outil d'autorisation de temporary white list, l'utilisateur doit exécuter l'applet **DeviceLock** du Panneau de configuration et sélectionner l'option **Temporary White List Authorization Tool**.

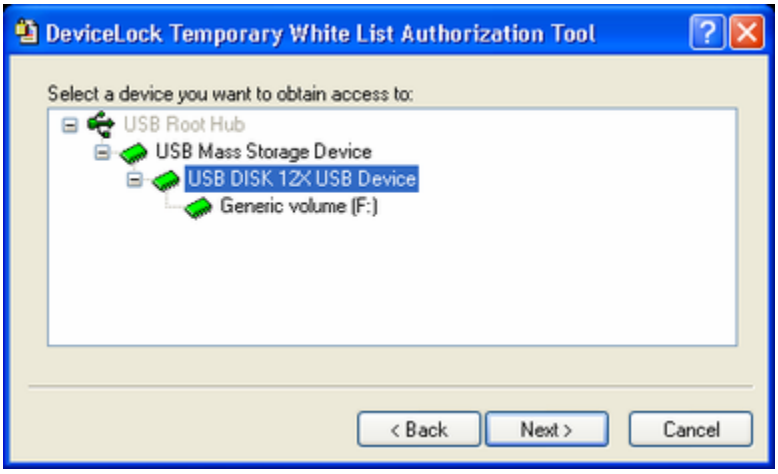


Remarque: Avec les versions XP et suivantes de Windows, l'utilisateur doit basculer en affichage classique du Panneau de configuration pour pouvoir afficher l'ensemble des applets disponibles.

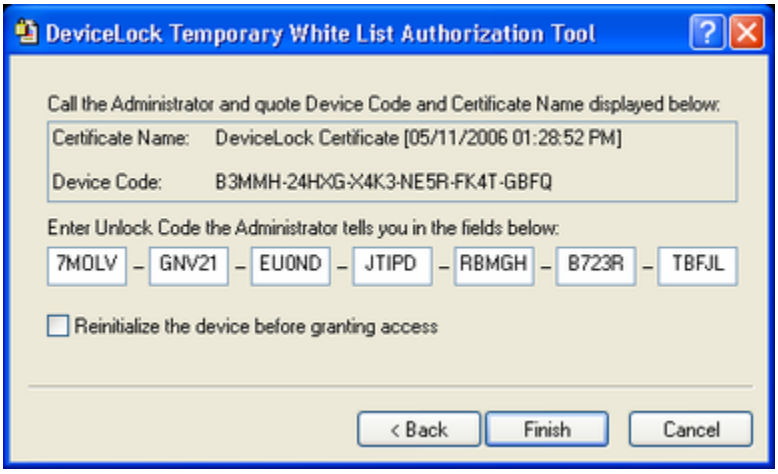

DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

Pour solliciter et obtenir l'accès temporaire à un périphérique, l'utilisateur doit effectuer cinq actions simples:

1. Brancher le périphérique considéré sur le port USB.
2. Sélectionner le périphérique dans la liste des périphériques USB disponibles.


DeviceLock Temporary White List Authorization Tool
Select a device you want to obtain access to:
USB Root Hub
USB Mass Storage Device
USB DISK 12X USB Device
Generic volume (F:)
< Back
Next >
Cancel

3. Contacter un administrateur et lui indiquer le nom du certificat et du **Device Code**. Veuillez noter que le **Device Code** a une durée de validité restreinte à 24 heures une fois généré par l'applet.


DeviceLock Temporary White List Authorization Tool
Call the Administrator and quote Device Code and Certificate Name displayed below:
Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]
Device Code: B3MMH-24HXG-X4K3-NE5R-FK4T-GBFQ
Enter Unlock Code the Administrator tells you in the fields below:
7MOLV – GNV21 – EU0ND – JTIPD – RBMGH – B723R – TBFJL
Reinitialize the device before granting access
< Back
Finish
Cancel

4. Saisir l'**Unlock Code** communiqué par l'administrateur.

   S'il s'avère nécessaire de réinitialiser (rebrancher) le périphérique avant d'y autoriser l'accès, sélectionnez **Reinitialize device before granting access**.

   Certains périphériques USB (comme la souris) ne fonctionneront pas sans réinitialisation. Il est donc conseillé de cocher cette case pour les périphériques autres que les dispositifs de stockage.

   Il est recommandé de ne pas cocher la case **Reinitialize device before granting access** pour les dispositifs de stockage (tels que les clés USB, les CD/DVD-ROM, les disques durs externes, etc.).

   Certains périphériques, dont les pilotes n'acceptent pas le rebranchement logiciel, ne peuvent pas être réinitialisés à partir de DeviceLock Service. Si un tel périphérique a été ajouté à la liste blanche mais ne fonctionne pas, l'utilisateur devra le débrancher et le rebrancher manuellement pour redémarrer le pilote du périphérique.

5. Appuyez sur le bouton **Finish**. Si l'**Unlock Code** est valide, l'accès au périphérique sera fourni en quelques secondes.

Toutes les tentatives réussies d'ajout de périphériques à une temporary white list sont répertoriées, si l'audit des modifications est activé dans les Service Options.

Annexe

Exemples d'autorisations et d'audit de périphériques

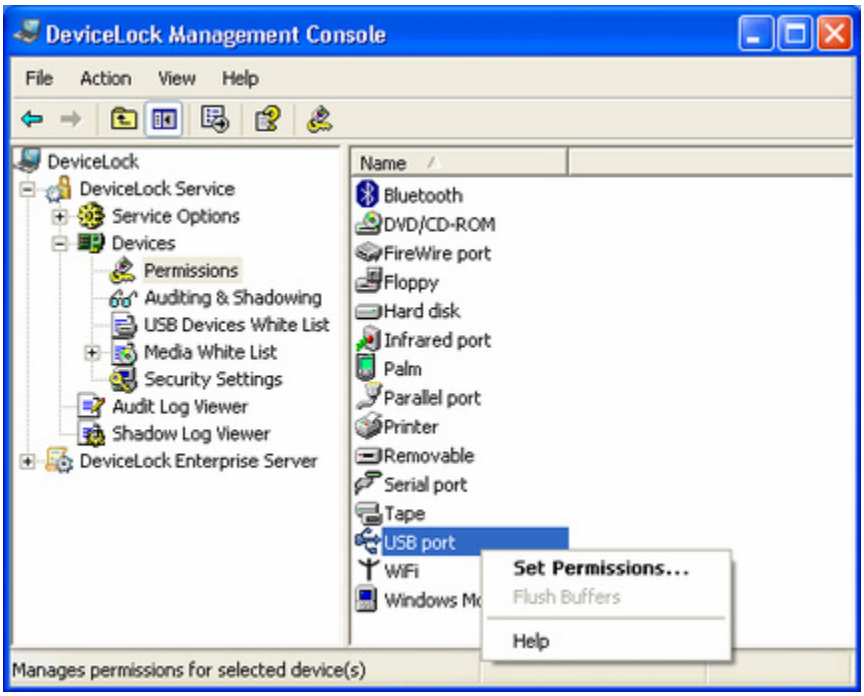
Les exemples suivants vous aideront à mieux comprendre comment définir correctement les autorisations et les règles d'audit et de réplication dans DeviceLock.

Tous les exemples partent du principe que vous utilisez la DeviceLock Management Console (l'extension MMC) et que celle-ci est déjà connectée à l'ordinateur qui exécute DeviceLock Service. Pour plus informations sur l'utilisation de la DeviceLock Management Console, veuillez lire la section DeviceLock Management Console de ce manuel.

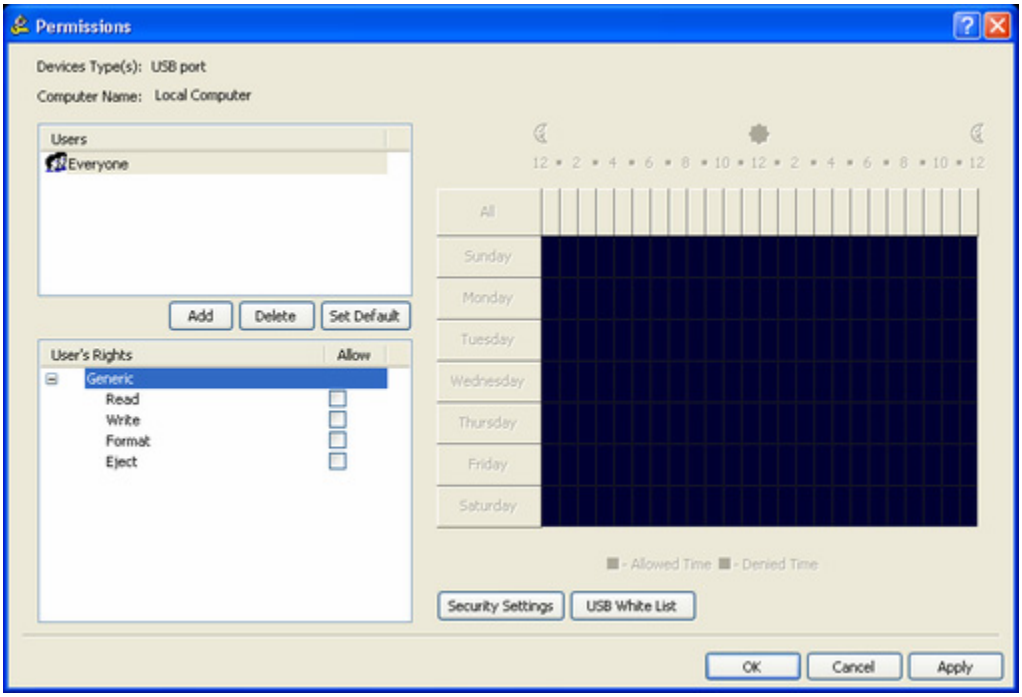
Exemples d'autorisations

Tous les périphériques USB sont interdits à l'ensemble des utilisateurs, sauf la souris et le clavier:

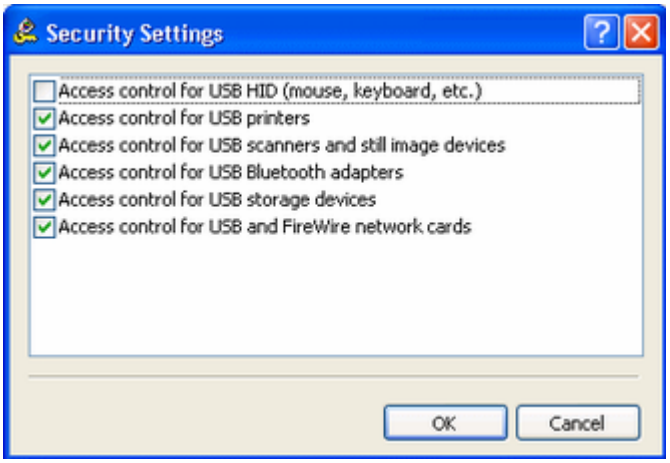
1. Sélectionnez l'élément **USB port** de la liste des types de périphériques dans **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.



2. Cliquez sur le bouton **Add** de la boîte de dialogue **Permissions**, ajoutez l'utilisateur **Everyone** (saisissez le nom ou consultez les noms disponibles et sélectionnez le nom recherché), cliquez sur **OK** pour refermer la boîte de dialogue **Select Users or Groups**, sélectionnez l'élément **Everyone** et désactivez tous les droits dans la liste des **User's Rights**.



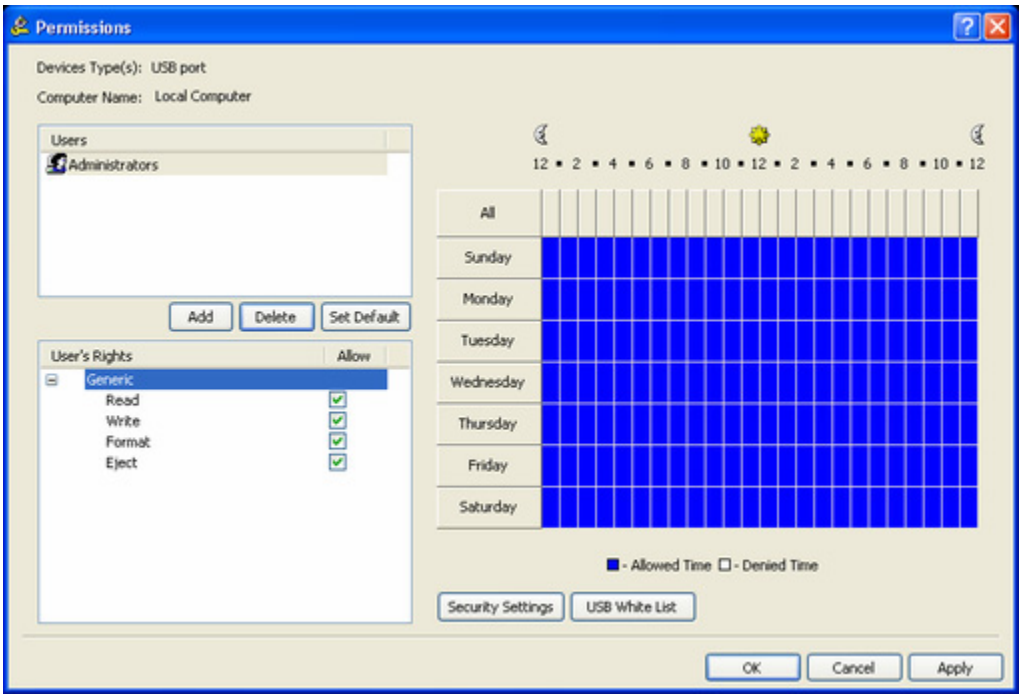
3. Cliquez sur **Security Settings** dans la boîte de dialogue **Permissions**, puis décochez **Access control for USB HID (mouse, keyboard, etc.)**, comme indiqué dans l’image ci-dessous.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

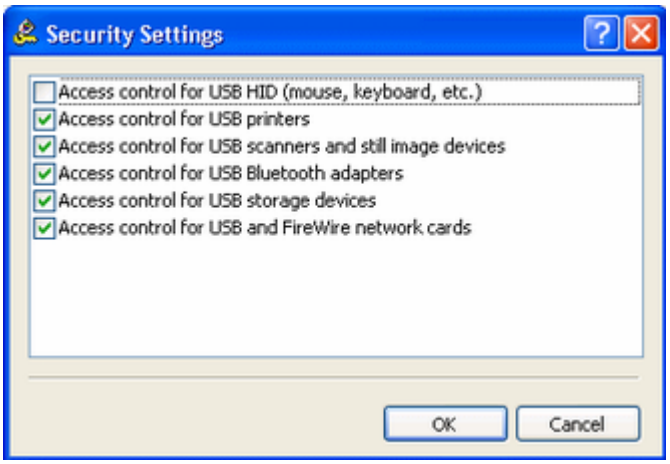
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Security Settings**, cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**, puis cliquez sur **Yes** pour confirmer votre volonté d'interdire l’accès au port USB à tous les utilisateurs.

Tous les périphériques USB sont interdits à l'ensemble des utilisateurs sauf la souris et le clavier, mais les membres du groupe Administrators peuvent utiliser les périphériques USB:

1. Sélectionnez l'élément **USB port** dans la liste des types de périphériques sous **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur le bouton **Add** de la boîte de dialogue **Permissions**, ajoutez le groupe **Administrators** (saisissez le nom ou consultez les noms disponibles et sélectionnez le nom recherché), cliquez sur **OK** pour refermer la boîte de dialogue **Select Users or Groups**, sélectionnez l'élément **Administrators** et activez tous les droits dans la liste des **User's Rights**.



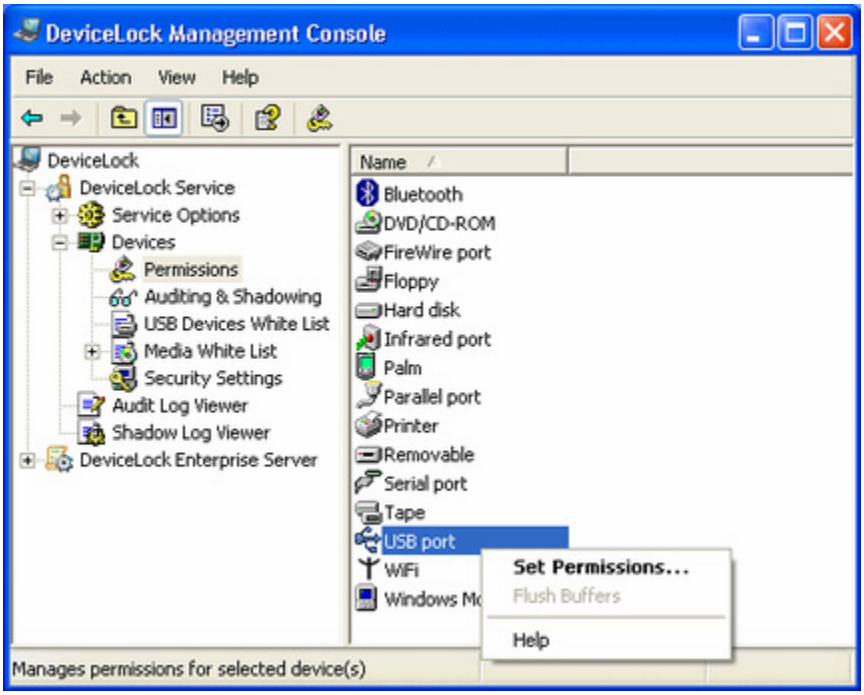
3. Cliquez sur **Security Settings** dans la boîte de dialogue **Permissions**, puis décochez **Access control for USB HID (mouse, keyboard, etc.)**, comme indiqué dans l'image ci-dessous.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

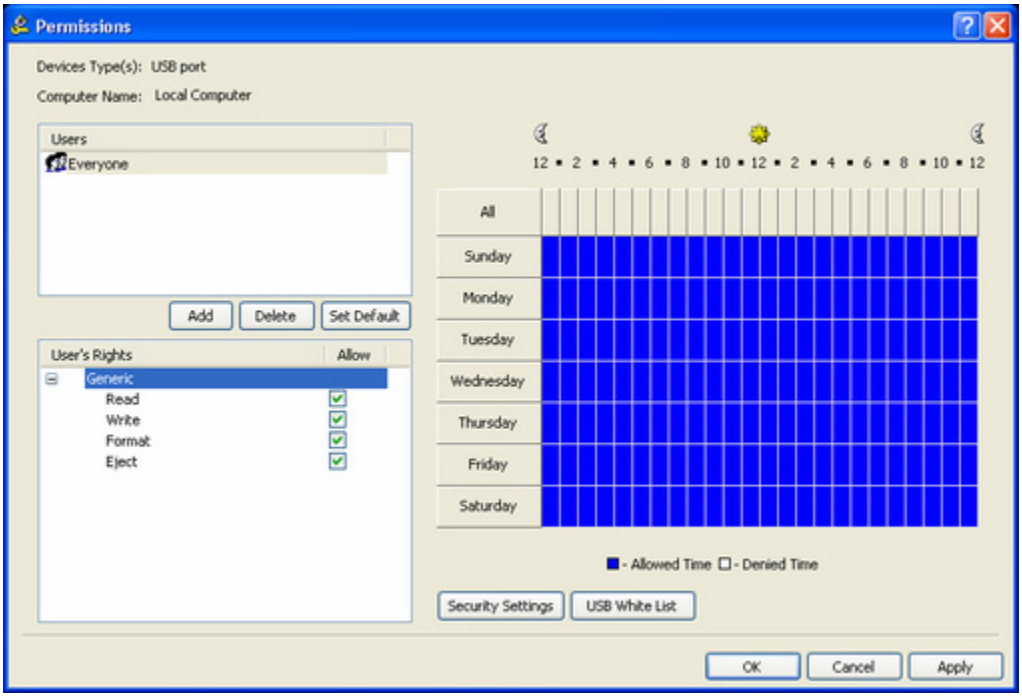
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Security Settings**, puis cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**.

Tous les dispositifs de stockage sont interdits à l'ensemble des utilisateurs sauf les disques durs non-amovibles, mais tous les périphériques USB qui ne servent pas au stockage sont autorisés:

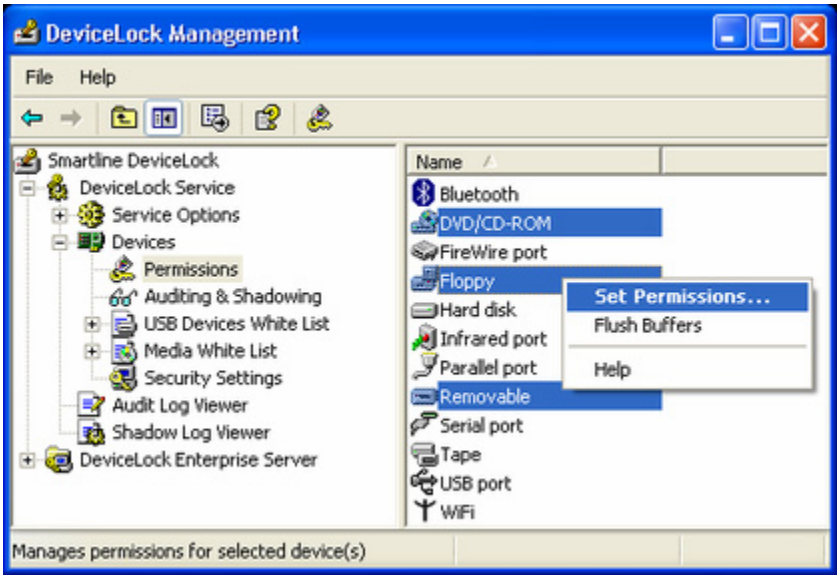
1. Sélectionnez l'élément **USB port** de la liste des types de périphériques sous **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.



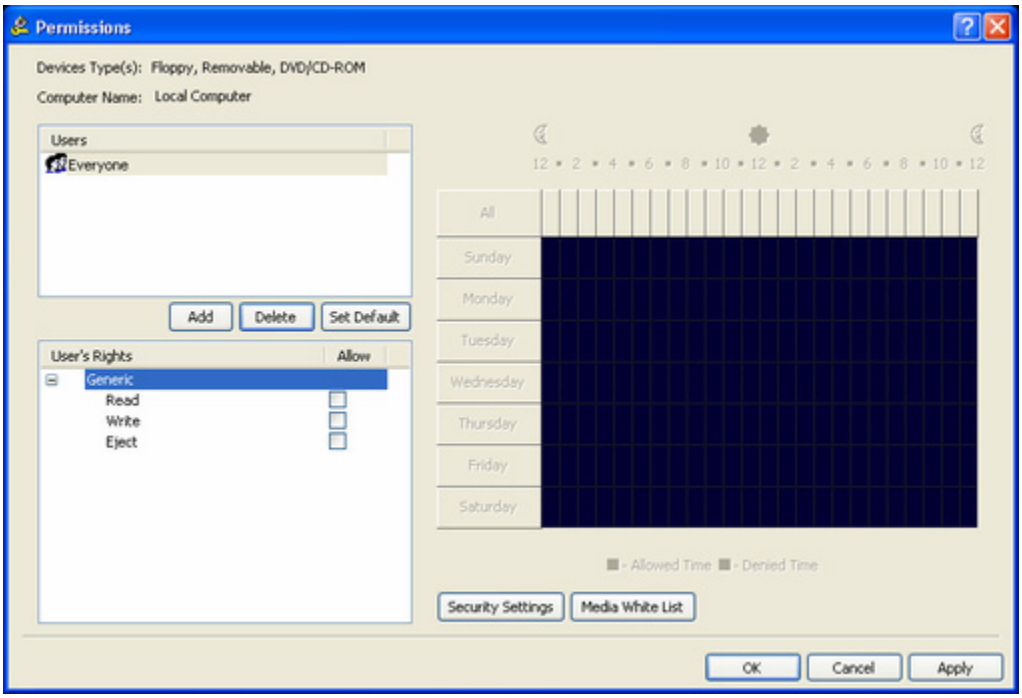
2. Cliquez sur le bouton **Add** de la boîte de dialogue **Permissions**, ajoutez le groupe **Everyone** (saisissez le nom ou consultez les noms disponibles et sélectionnez le nom recherché), cliquez sur **OK** pour refermer la boîte de dialogue **Select Users or Groups**, sélectionnez l'élément **Everyone** et activez tous les droits dans la liste des **User's Rights**.



3. Cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**.
4. Sélectionnez les éléments **DVD/CD-ROM**, **Floppy** et **Removable** de la liste des types de périphériques dans **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.



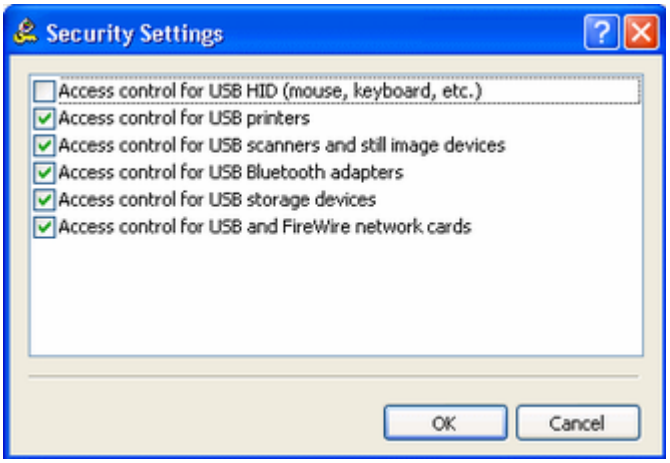
5. Cliquez sur le bouton **Add** de la boîte de dialogue **Permissions**, ajoutez le groupe **Everyone** (saisissez le nom ou consultez les noms disponibles et sélectionnez le nom recherché), cliquez sur **OK** pour refermer la boîte de dialogue **Select Users or Groups**, sélectionnez l'élément **Everyone** et activez tous les droits dans la liste des **User's Rights**.



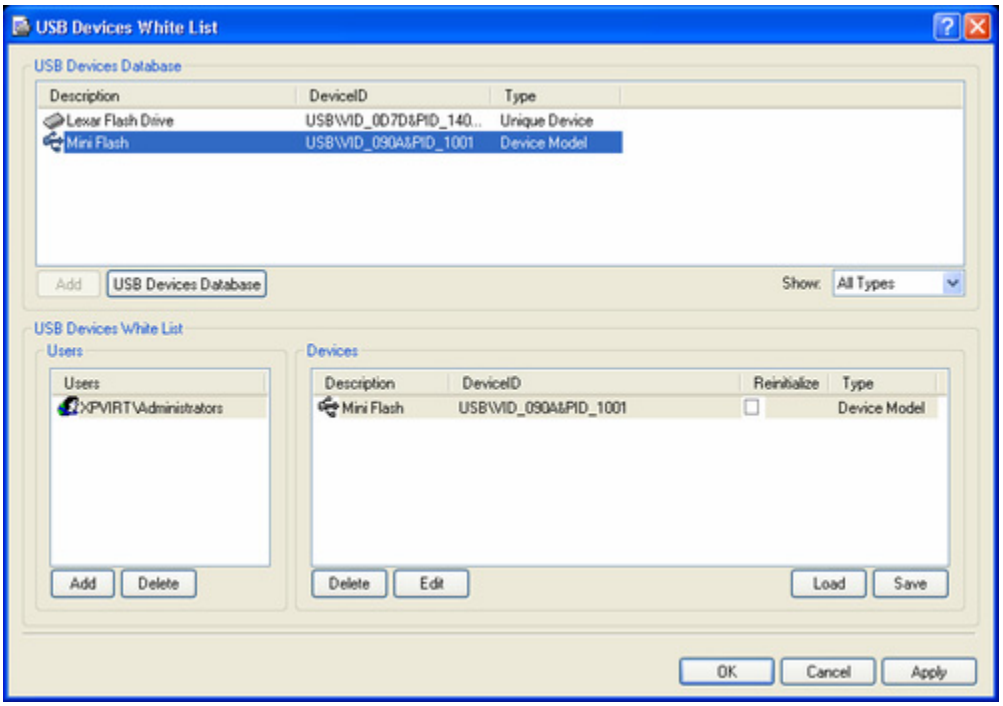
6. Cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**, puis cliquez sur **Yes** pour confirmer votre volonté d'interdire l'accès à ces périphériques à tous les utilisateurs.

Tous les périphériques USB sont interdits à l'ensemble des utilisateurs sauf la souris et le clavier, mais les membres du groupe Administrators peuvent utiliser un modèle autorisé de périphérique de stockage USB:

1. Sélectionnez l'élément **USB port** de la liste des types de périphériques sous **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur **Add** dans la boîte de dialogue **Permissions** et ajoutez l'utilisateur **Everyone** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez **Everyone** et désactivez **User's Rights** dans la liste.
3. Cliquez sur **Security Settings** dans la boîte de dialogue **Permissions**, puis décochez **Access control for USB HID (mouse, keyboard, etc.)**, comme indiqué dans l'image ci-dessous.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Security Settings**, puis cliquez sur **USB White List** dans la boîte de dialogue **Permissions**.



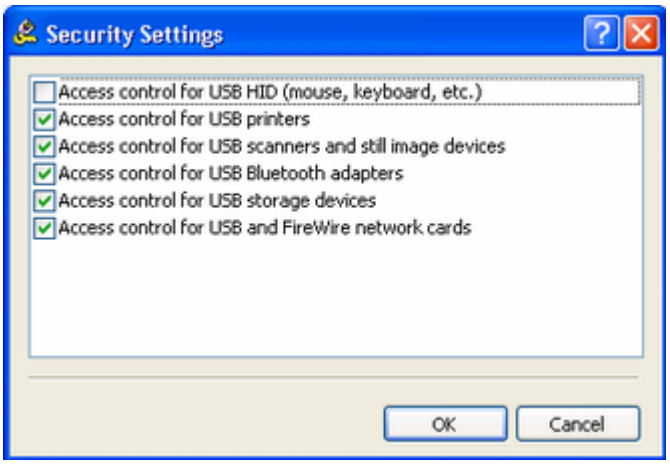
5. Cliquez sur **Add** sous la liste Users, ajoutez le groupe **Administrators** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient), cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups** et sélectionnez **Administrators**.
6. Sélectionnez le modèle du périphérique dans la liste **USB Devices Database**, puis cliquez sur **Add**, sous cette liste.

   Si vos périphériques ne figurent pas dans la base de données des périphériques USB, cliquez sur **USB Devices Database** sous la liste, puis rajoutez les périphériques comme indiqué dans le chapitre USB Devices Database. Lorsque vous avez terminé de rajouter des périphériques dans la base, cliquez sur **OK** pour l'enregistrer, et pour fermer la boîte de dialogue **USB Devices Database**.

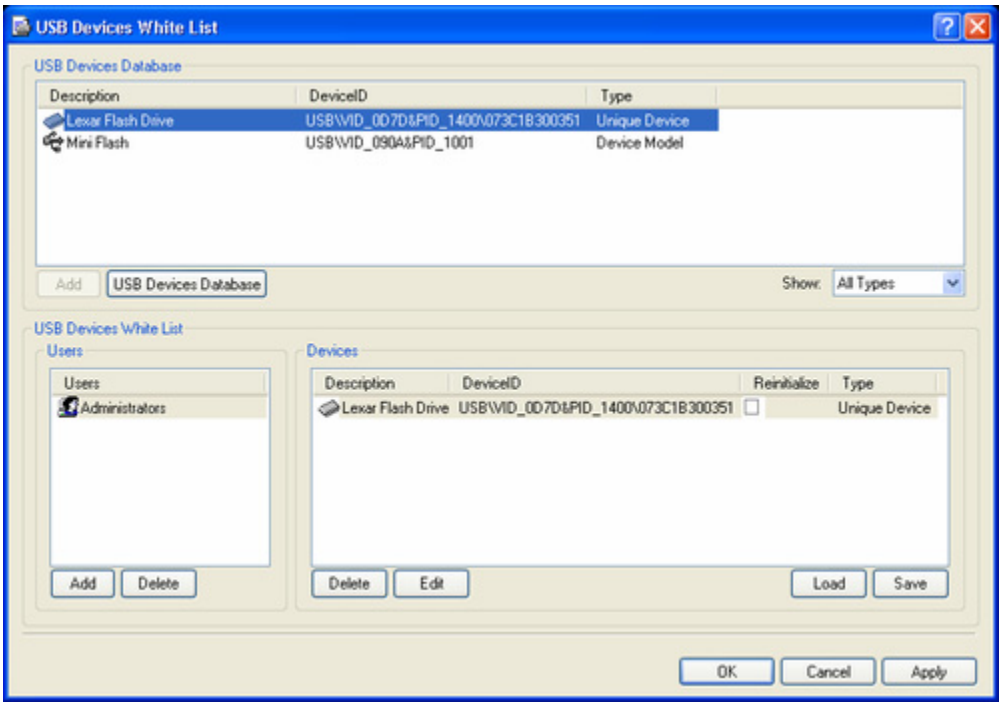
7. Cliquez sur **OK** pour appliquer les paramètres de la liste blanche et fermer la boîte de dialogue de **USB Devices White List**, cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**, puis cliquez sur **Yes** pour confirmer votre volonté d'interdire l'accès au port USB à tous les utilisateurs.

Tous les périphériques USB sont interdits à l'ensemble des utilisateurs sauf la souris et le clavier, mais les membres du groupe Administrators peuvent utiliser un périphérique unique autorisé de stockage USB:

1. Sélectionnez l'élément **USB port** de la liste des types de périphériques sous **Permissions**, puis choisissez l'option **Set Permissions** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur **Add** dans la boîte de dialogue **Permissions** et ajoutez l'utilisateur **Everyone** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez **Everyone** et désactivez **User's Rights** dans la liste.
3. Cliquez sur **Security Settings** dans la boîte de dialogue **Permissions**, puis décochez **Access control for USB HID (mouse, keyboard, etc.)**, comme indiqué dans l'image ci-dessous.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Security Settings**, puis cliquez sur **USB White List** dans la boîte de dialogue **Permissions**.



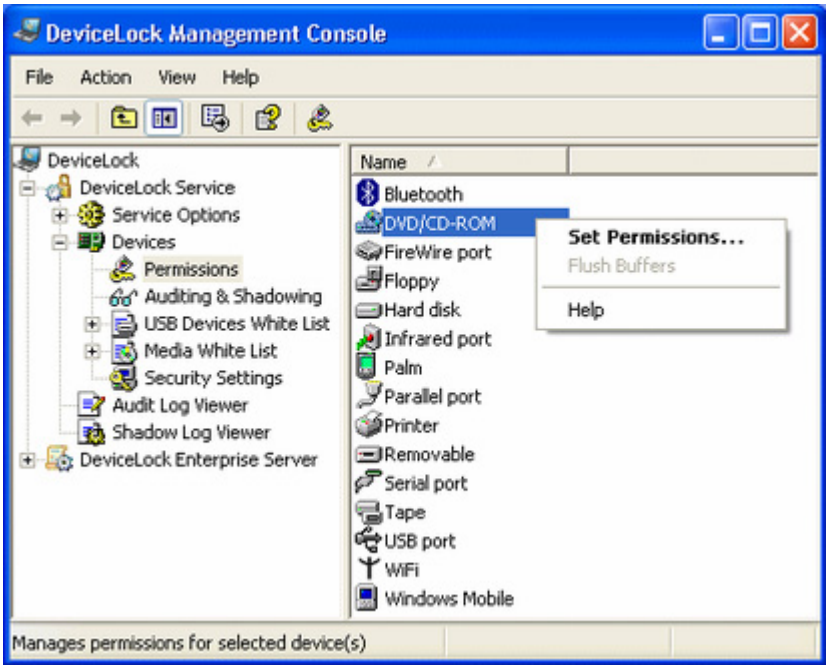
5. Cliquez sur **Add** sous la liste Users, ajoutez le groupe **Administrators** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient), cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups** et sélectionnez **Administrators**.
6. Sélectionnez le périphérique unique dans la liste **USB Devices Database**, puis cliquez sur **Add**, sous cette liste.

   Si vos périphériques ne figurent pas dans la base de données des périphériques USB, cliquez sur **USB Devices Database** sous la liste, puis rajoutez les périphériques comme indiqué dans le chapitre USB Devices Database. Lorsque vous avez terminé de rajouter des périphériques dans la base, cliquez sur **OK** pour l’enregistrer, et pour fermer la boîte de dialogue **USB Devices Database**.

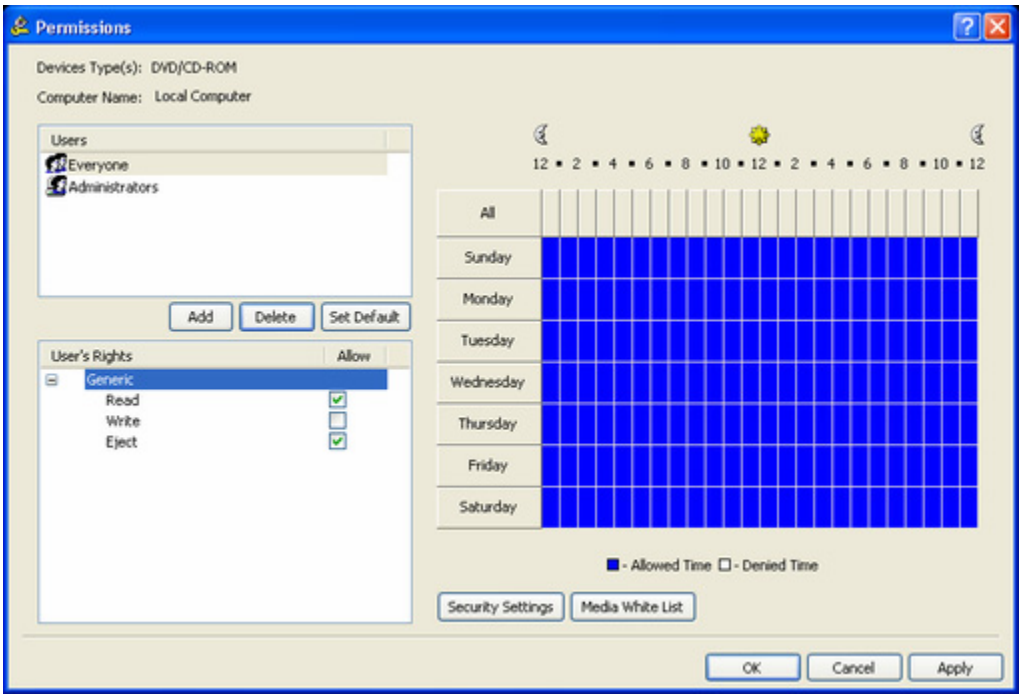
7. Cliquez sur **OK** pour appliquer les paramètres de la liste blanche et fermer la boîte de dialogue de **USB Devices White List**, cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**, puis cliquez sur **Yes** pour confirmer votre volonté d'interdire l’accès au port USB à tous les utilisateurs.

Les lecteurs CD et DVD ne sont accessibles qu'en lecture seule à l’ensemble des utilisateurs, mais les membres du groupe Administrators peuvent graver (écrire) des disques CD et DVD:

1. Sélectionnez l’élément **DVD/CD-ROM** de la liste des types de périphériques dans **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d’un simple clic droit.



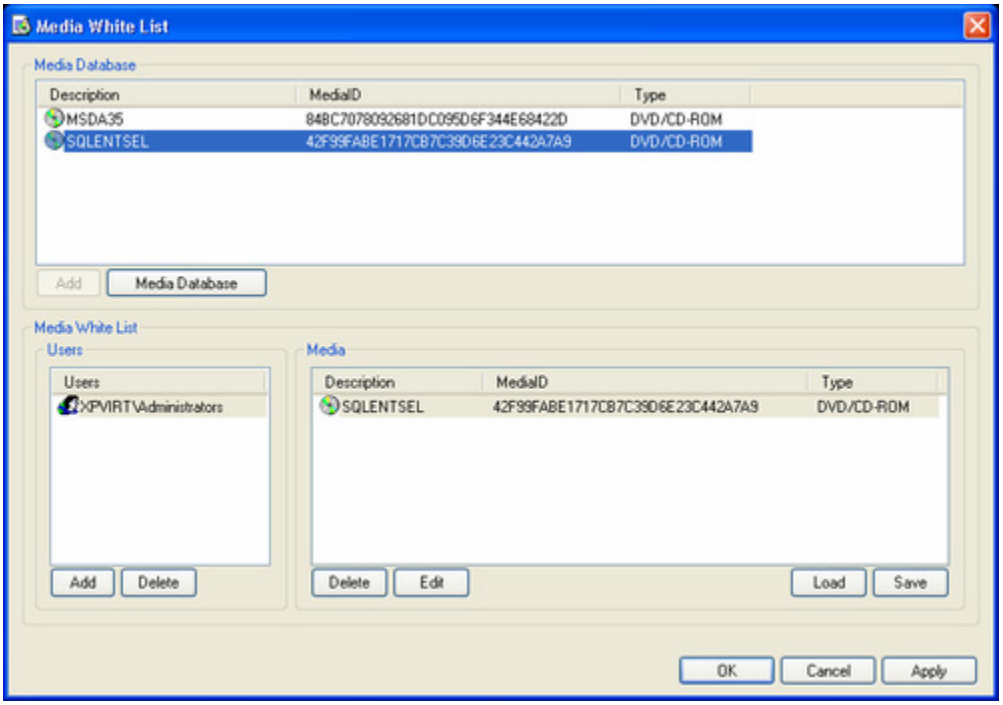
2. Cliquez sur **Add** dans la boîte de dialogue **Permissions** et ajoutez le groupe **Administrators** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez **Everyone** et désactivez **User's Rights** dans la liste.
3. Cliquez sur **Add** dans la boîte de dialogue **Permissions** et ajoutez l'utilisateur **Everyone** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**. Sélectionnez l'élément **Everyone** et désactivez le droit **Write** dans la liste des **User's Rights**.



4. Cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue de **Permissions**.

Les lecteurs CD et DVD sont interdits à l'ensemble des utilisateurs, mais les membres du groupe Administrators peuvent lire un disque en particulier:

1. Sélectionnez l'élément **DVD/CD-ROM** de la liste des types de périphériques sous **Permissions**, puis choisissez **Set Permissions** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur **Add** dans la boîte de dialogue **Permissions** et ajoutez l'utilisateur **Everyone** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez **Everyone** est désactivez tous les droits dans la liste des **User's Rights**.
3. Cliquez sur **Media White List** dans la boîte de dialogue **Permissions**.



4. Cliquez sur **Add** sous la liste **Users**, ajoutez le groupe **Administrators** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient), cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups** et sélectionnez **Administrators**.
5. Sélectionnez le média dans la liste **Media Database**, puis cliquez sur **Add**, sous cette liste.

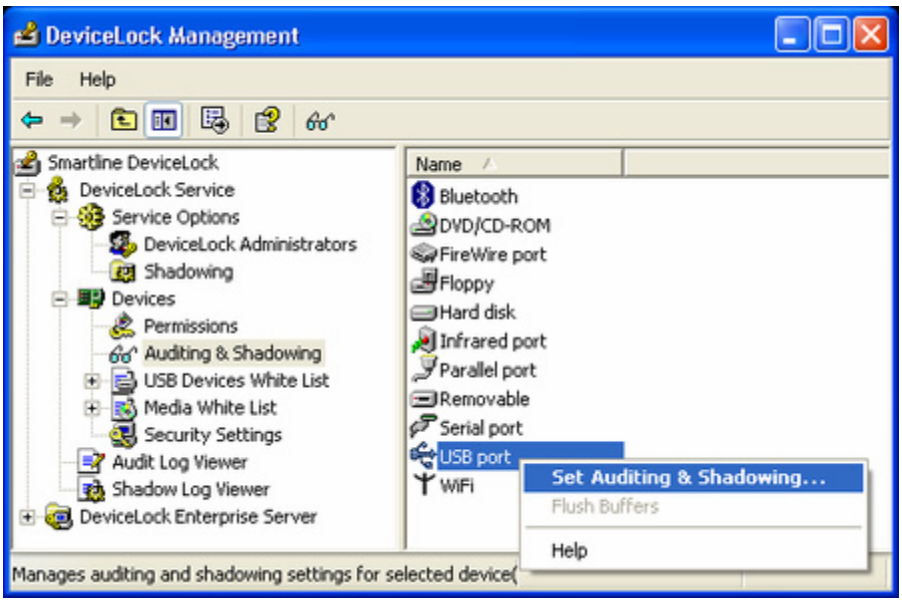
   Si vos disques ne figurent pas dans la base de données des médias, cliquez sur **Media Database** sous la liste, puis autorisez un média comme indiqué dans le chapitre Media Database. Lorsque vous avez terminé d'autoriser des médias, cliquez sur **OK** pour enregistrer la base de données et fermer la boîte de dialogue **Media Database**.

6. Cliquez sur **OK** pour appliquer les paramètres de la liste blanche et fermer la boîte de dialogue de **Media White List**, cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Permissions**, puis cliquez sur **Yes** pour confirmer votre volonté d'interdire l'accès aux lecteurs CD/DVD à tous les utilisateurs.

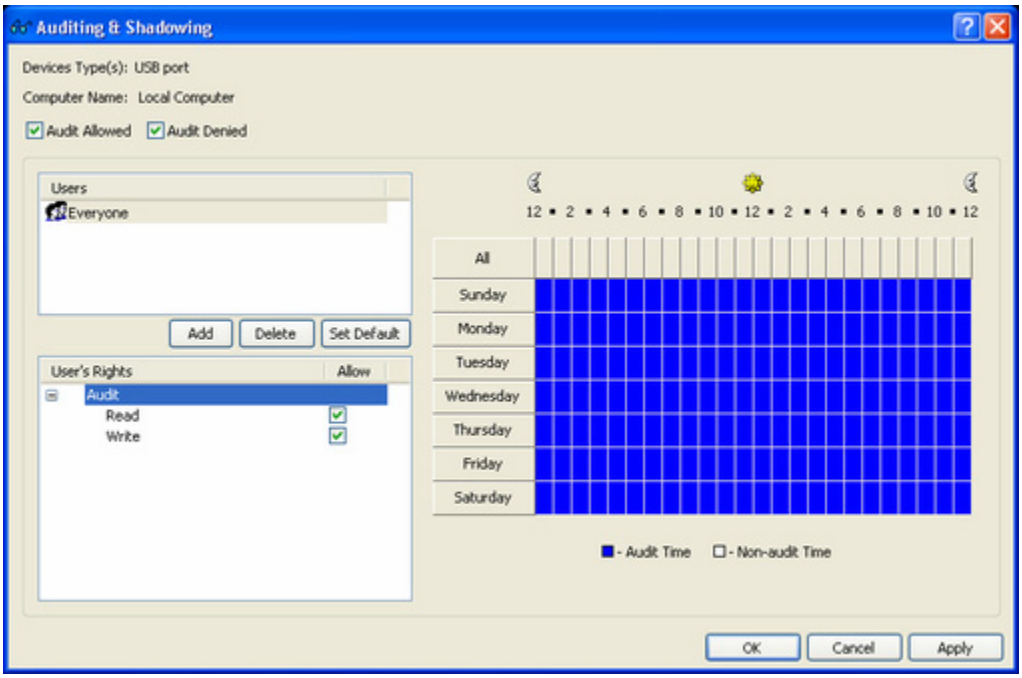
Exemples de règles d'audit et de réplication

Enregistrer les actions insérer, retirer et accéder pour les périphériques USB et pour tous les utilisateurs.

1. Sélectionnez l'élément **USB port** dans la liste des types de périphériques sous **Auditing & Shadowing**, puis choisissez l'option **Set Auditing & Shadowing** du menu contextuel disponible d'un simple clic droit.



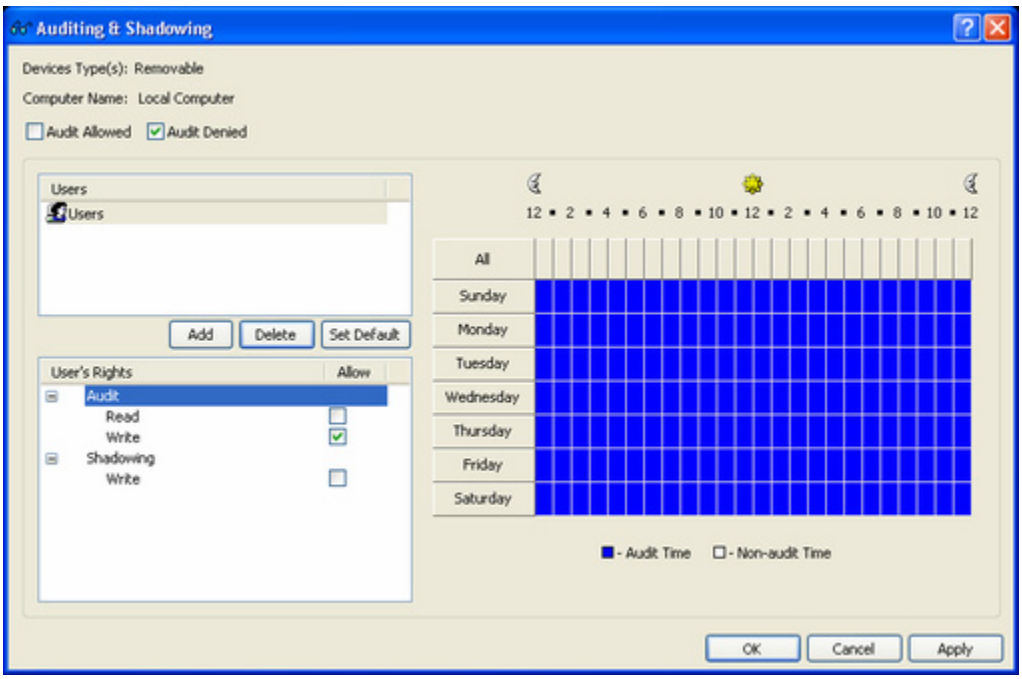
2. Cliquez sur le bouton **Add** de la fenêtre **Audit** et ajoutez l'utilisateur **Everyone** (tapez le nom ou parcourez les noms disponibles et sélectionnez le nom qui vous convient). Cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez l'élément **Everyone** et activez les droits d'audit **Read** et **Write** dans la liste des **User's Rights**.



3. Cochez **Audit Allowed** et **Audit Denied** en haut de la boîte de dialogue **Auditing & Shadowing**, puis cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Auditing & Shadowing**.

N'enregistrer que les noms des fichiers et dossiers ayant trait aux essais d'écriture refusés pour les dispositifs de stockage amovibles et les membres du groupe Users:

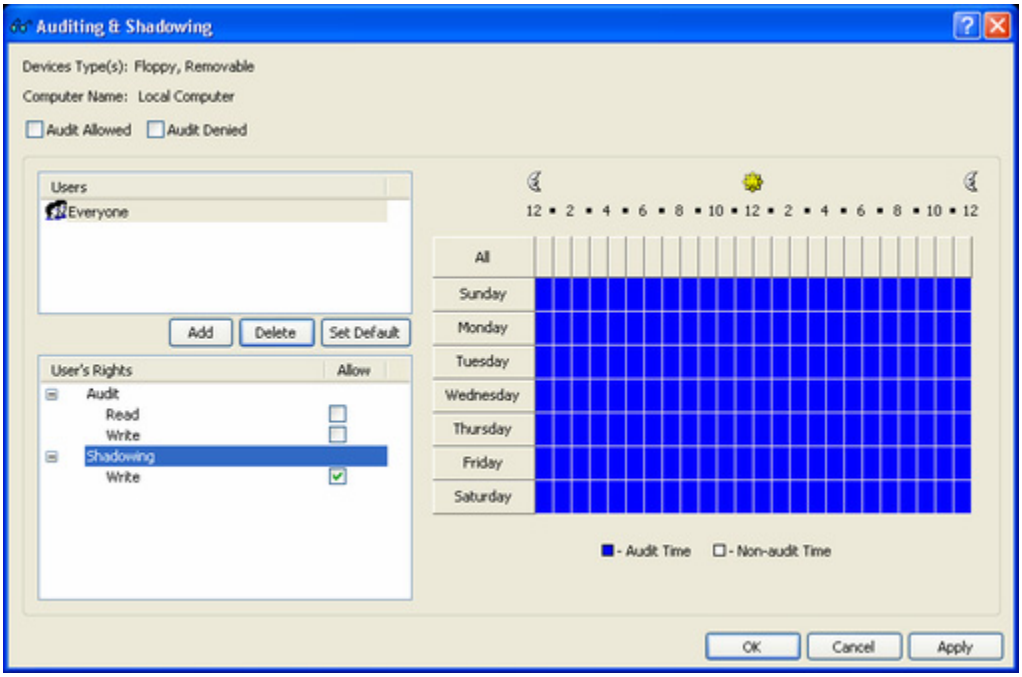
1. Sélectionnez l'élément **Removable** dans la liste des types de périphériques sous **Auditing & Shadowing**, puis choisissez **Set Auditing & Shadowing** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur l'option **Add** de la boîte de dialogue **Auditing & Shadowing**, ajoutez le groupe **Users** (tapez le nom ou parcourez les noms disponibles et sélectionnez celui qui vous convient), cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups**, sélectionnez **Users** et sélectionnez **Audit Write** dans la liste déroulante.



3. Cochez uniquement **Audit Denied** en haut de la boîte de dialogue **Auditing & Shadowing**, puis cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Auditing & Shadowing**.

Répliquez toutes les données transférées vers des dispositifs de stockage amovibles et vers des disquettes, et ce pour tous les utilisateurs:

1. Sélectionnez les éléments **Floppy** et **Removable** dans la liste des types de périphériques sous **Auditing & Shadowing**, puis choisissez l'option **Set Auditing & Shadowing** du menu contextuel disponible d'un simple clic droit.
2. Cliquez sur **Add** dans la boîte de dialogue **Auditing & Shadowing**, ajoutez l'utilisateur **Everyone**, cliquez sur **OK** pour fermer la boîte de dialogue **Select Users or Groups** et sélectionnez **Everyone**. Dans la liste déroulante, sélectionnez **No Audit** et cochez la case **Enable Write Shadowing**.

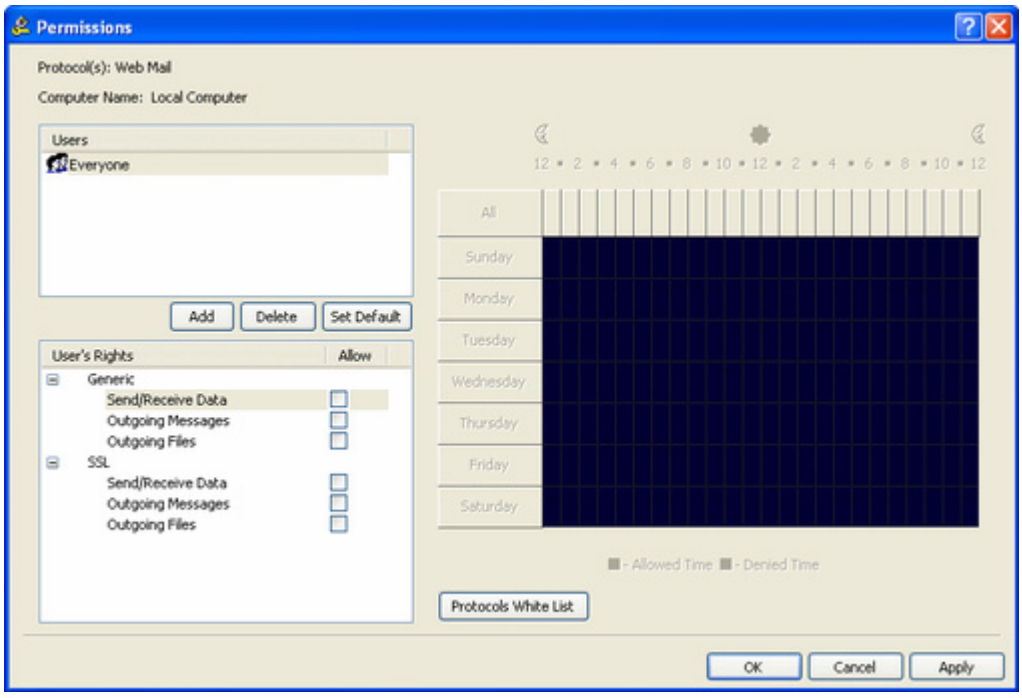


3. Cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue **Auditing & Shadowing**.

Exemples d’autorisations de protocoles

Pour tous les utilisateurs, tous les services de messagerie sont refusés, mais les membres du groupe Administrators peuvent accéder à Gmail:

1. Dans l'arborescence, développez **DeviceLock Service**, puis **Protocols**.
2. Dans **Protocols**, sélectionnez **Permissions**.
3. Dans le panneau de détails, cliquez droit sur **Web Mail**, puis cliquez sur **Set Permissions**.
4. Dans la boîte de dialogue **Permissions**, procédez comme suit:
   a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Everyone** puis cliquez sur **OK**.
   b) Dans **Users**, sélectionnez **Everyone**.
   c) Dans **User’s Rights**, décochez toutes les cases pour désactiver tous les droits.

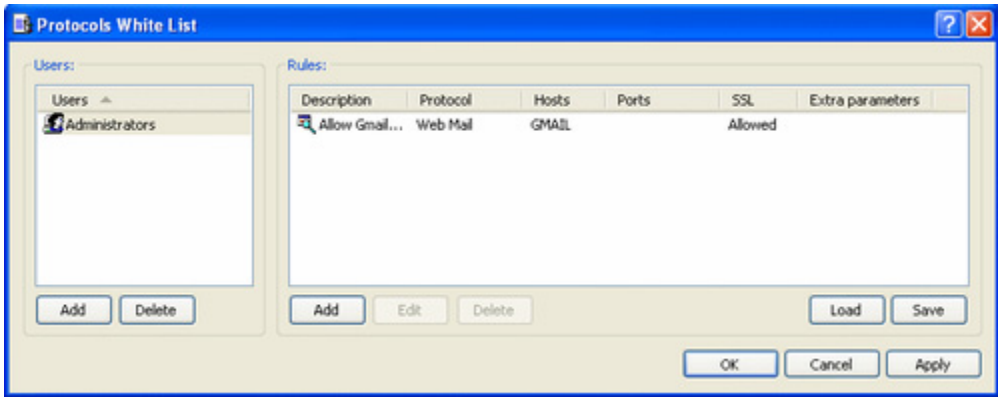


d) Cliquez sur **Protocols White List**.

5. Dans la boîte de dialogue **Protocols White List**, procédez comme suit:

   a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Administrators** puis cliquez sur **OK**.

   b) Dans **Users**, sélectionnez **Administrators** puis, dans **Rules**, cliquez sur **Add**. Dans le champ **Description** de la boîte de dialogue **Add Rule**, indiquez le nom de la règle. Ensuite, dans **Web Mail services**, cochez la case **Gmail** puis cliquez sur **OK**.

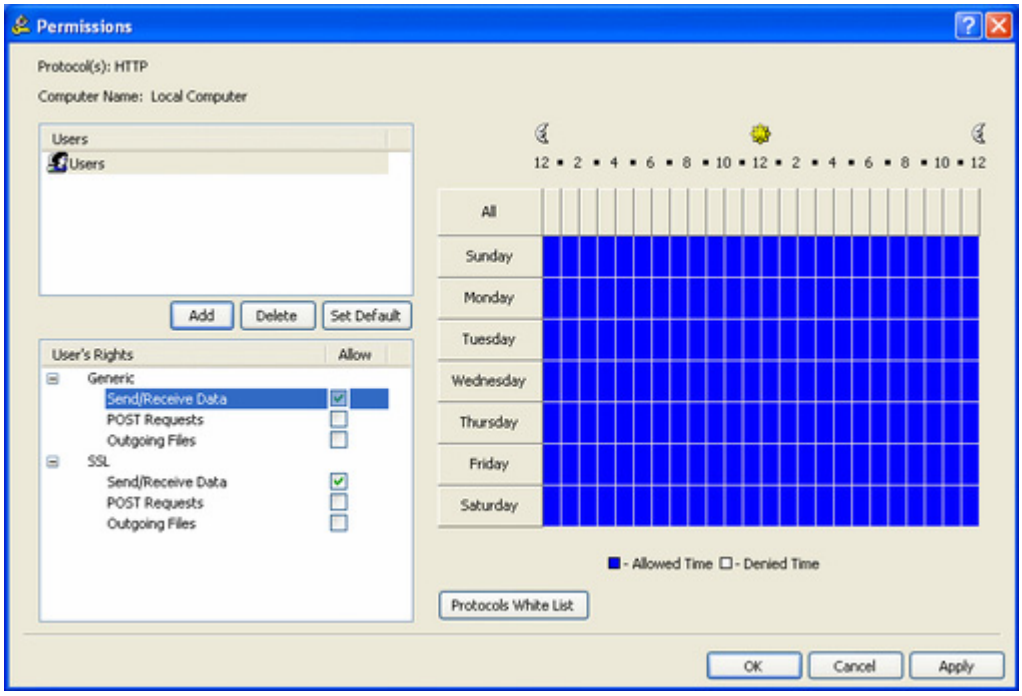


   c) Cliquez sur **OK** ou **Apply** pour appliquer les paramètres de la liste blanche et fermez la boîte de dialogue **Protocols White List**.

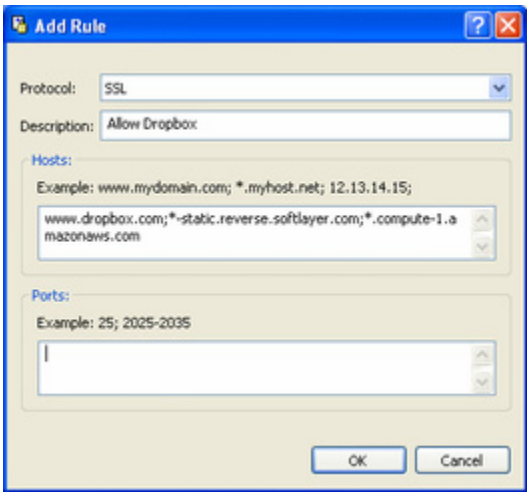
6. Dans la boîte de dialogue **Permissions**, cliquez sur **OK** ou **Apply**.

Les membres du groupe Users sont autorisés à utiliser Dropbox:

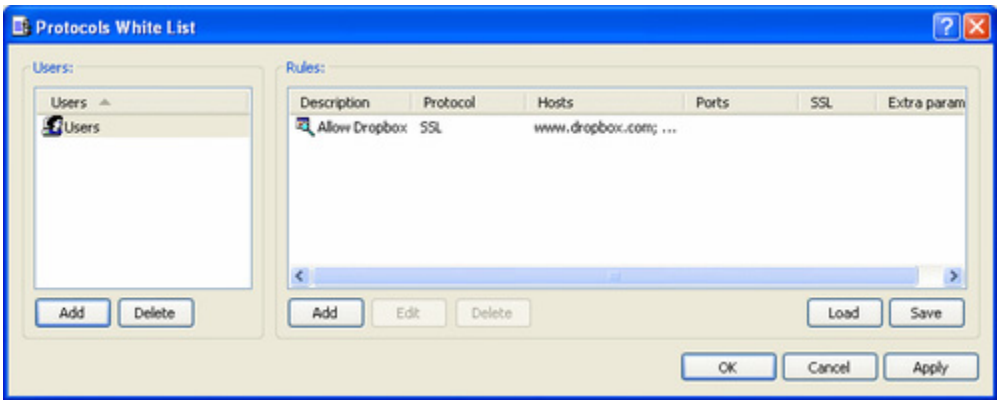
1. Dans l'arborescence, développez **DeviceLock Service**, puis **Protocols**.
2. Dans **Protocols**, sélectionnez **Permissions**.
3. Dans le panneau de détails, cliquez droit sur **HTTP**, puis cliquez sur **Set Permissions**.
4. Dans la boîte de dialogue **Permissions**, procédez comme suit:
   a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Users** puis cliquez sur **OK**.
   b) Dans **Users**, sélectionnez **Users**.
   c) Dans **User's Rights**, cochez les cases situées en regard des droits suivants: **Generic: Send/Receive Data** et **SSL: Send/Receive Data**.



   d) Cliquez sur **Protocols White List**.
5. Dans la boîte de dialogue **Protocols White List**, procédez comme suit:
   a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Users** puis cliquez sur **OK**.
   b) Dans **Users**, sélectionnez **Users** puis, dans **Rules**, cliquez sur **Add**.
6. Dans la boîte de dialogue **Add Rule**, procédez comme suit:
   a) Dans la liste **Protocol:** cliquez sur **SSL**.
   b) Dans le champ **Description**, indiquez le nom de la règle.
   c) Dans le champ **Hosts:**, saisissez les noms DNS des serveurs Dropbox séparés par une virgule ou un point-virgule: **www.dropbox.com; *-static.reverse.softlayer.com; *.compute-1.amazonaws.com**.



d) Cliquez sur **OK**.



7. Cliquez sur **OK** ou **Apply** pour appliquer les paramètres de la liste blanche et fermez la boîte de dialogue **Protocols White List**.
8. Dans la boîte de dialogue **Permissions**, cliquez sur **OK** ou **Apply**.

Remarque: Le contrôle d'accès, l'audit, la réplication et le filtrage de contenu seront désactivés pour tous les transferts de fichiers Dropbox.

Exemples de règles contextuelles

Tous les utilisateurs se voient refusé le droit de copier vers des périphériques (disquettes, amovibles) et de transmettre sur le réseau (via http, FTP, SMTP, messagerie Web) les types de contenu suivants : les fichiers contenant plus d'un numéro de carte de crédit, les documents et les archives protégés par mot de passe, les fichiers contenant plus d'un numéro de sécurité sociale, et les images contenant une grande quantité de texte.

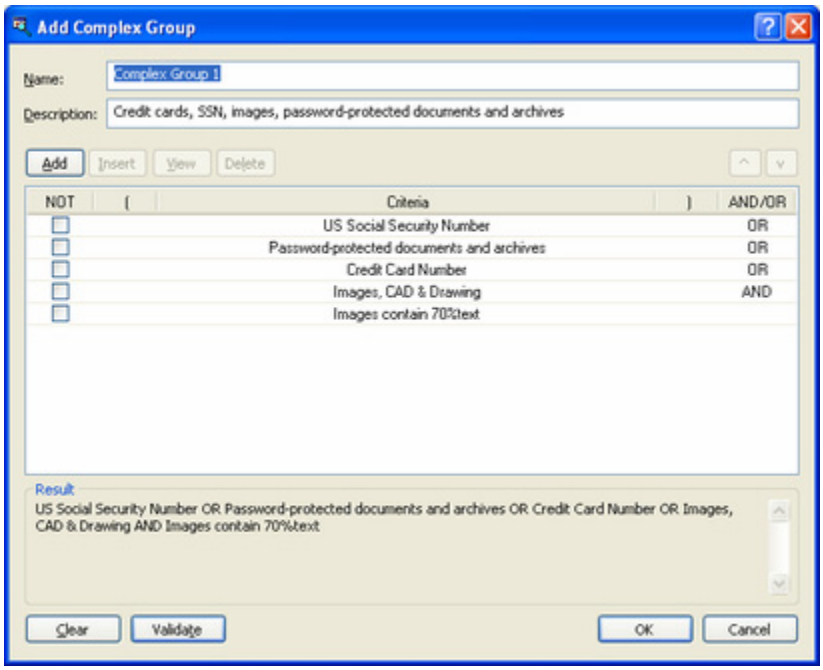
1. Dans l'arborescence de console, développez **DeviceLock Service**, puis **Devices**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.

2. Dans le champ **Content Database** de la boîte de dialogue **Content-Aware Rules for Devices**, cliquez sur la flèche déroulante située en regard de l'option **Add Group**, puis cliquez sur **Document Properties**.
3. Dans la boîte de dialogue **Add Document Properties Group**, effectuez la chose suivante:
    a) Dans le champ **Name**, indiquez le nom du groupe, par exemple **Password-protected documents and archives**.
    b) Cochez la case **Password protected**.
    c) Cliquez sur **OK**.

    Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database de la boîte de dialogue Content-Aware Rules for Devices. Ce groupe servira à contrôler l'accès aux documents et archives protégés par mot de passe.
4. Dans le champ **Content Database** de la boîte de dialogue **Content-Aware Rules for Devices**, cliquez sur la flèche déroulante située en regard de l'option **Add Group**, puis cliquez sur **Document Properties**.
5. Dans la boîte de dialogue **Add Document Properties Group**, effectuez la chose suivante:
    a) Dans le champ **Name**, indiquez le nom du groupe, par exemple **Images contain 70%text**.
    b) Cochez la case **Contains text** et indiquez **70 %**.
    c) Cliquez sur **OK**.

    Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database de la boîte de dialogue Content-Aware Rules for Devices. Ce groupe servira à contrôler l'accès aux images contenant une grande quantité de texte.
6. Dans le champ **Content Database** de la boîte de dialogue **Content-Aware Rules for Devices**, cliquez sur la flèche déroulante située en regard de l'option **Add Group**, puis cliquez sur **Complex**.
7. Dans la boîte de dialogue **Add Complex Group**, procédez comme suit:
    a) Dans le champ **Name**, indiquez le nom du groupe, par exemple **Complex Group 1**.
    b) Cliquez sur **Add**. Dans la boîte de dialogue **Content Groups**, sélectionnez les groupes suivants: **Credit Card Number**, **Images, CAD & Drawing**, **Images contain 70%text**, **Password-protected documents and archives**, et **US Social Security Number**.

    Pour sélectionner ces groupes simultanément, appuyez sur la touche CTRL tout en cliquant dessus.
    c) Composer l'expression logique suivante: **US Social Security Number OR Password-protected documents and archives OR Credit Card Number OR Images, CAD & Drawing AND Images contain 70%text**.

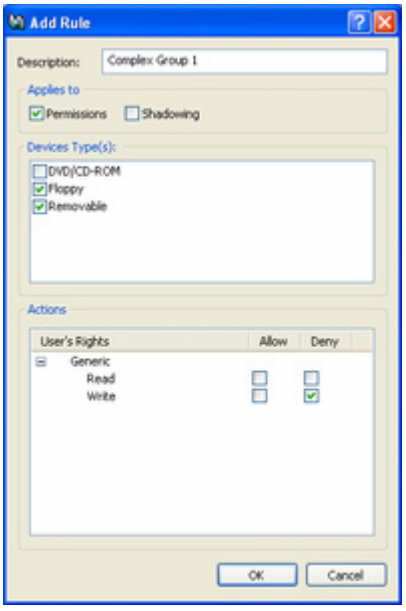


d) Cliquez sur **OK**.

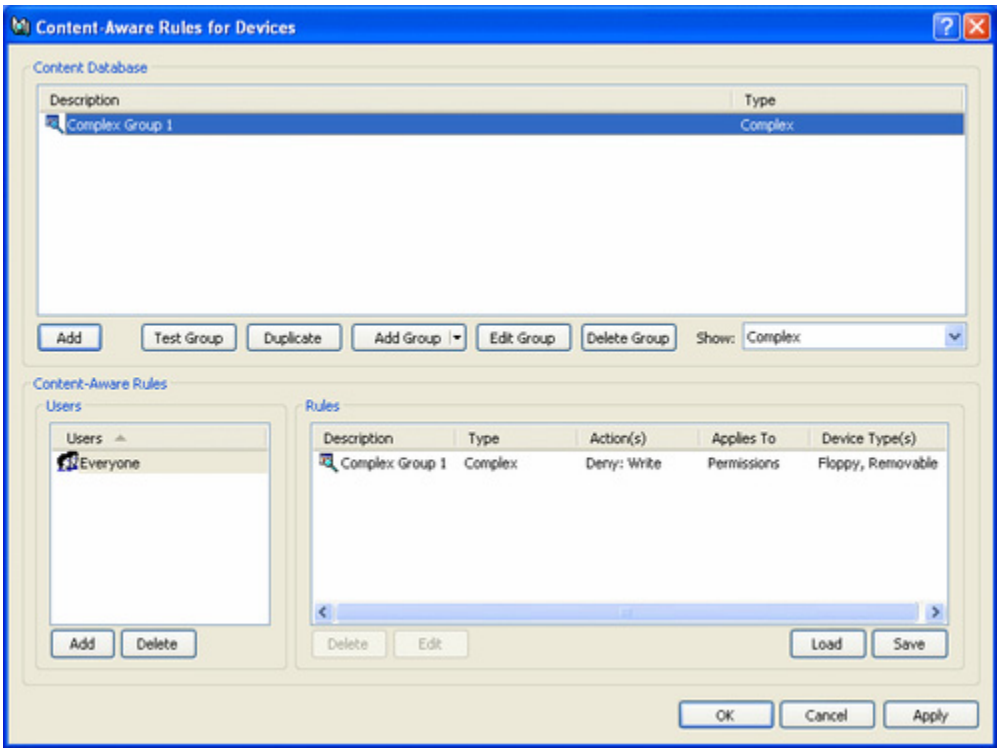
Le nouveau groupe de contenus ainsi créé est ajouté à la liste des groupes de contenus existante dans le champ Content Database de la boîte de dialogue Content-Aware Rules for Devices. Ce groupe servira à contrôler l'accès aux fichiers contenant plus d'un numéro de carte de crédit, les documents et les archives protégés par mot de passe, les fichiers contenant plus d'un numéro de sécurité sociale, et les images contenant une grande quantité de texte.

8. Dans la boîte de dialogue **Content-Aware Rules for Devices**, procédez comme suit:
   a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Everyone** puis cliquez sur **OK**.
   b) Dans **Users**, sélectionnez **Everyone**. Dans **Content Database**, sélectionnez le groupe de contenus **Complex Group 1**, puis cliquez sur **Add**.
9. Dans la boîte de dialogue **Add Rule**, procédez comme suit:
   a) Dans **Applies to**, cochez la case **Permissions**.
   b) Dans **Device Type(s)**, cochez les cases **Floppy** et **Removable**.

c) Dans **Action(s)**, cochez la case **Deny** située en regard du champ **Write**.

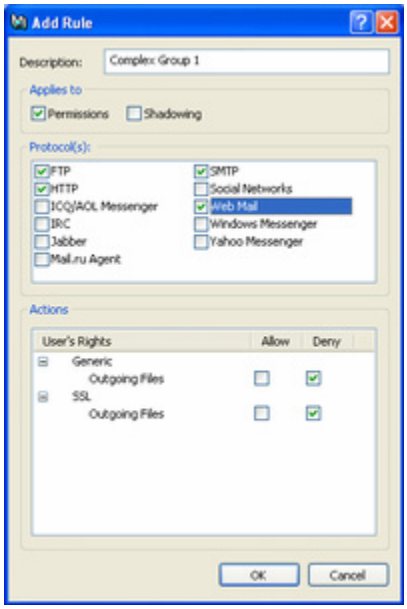


d) Cliquez sur **OK**.

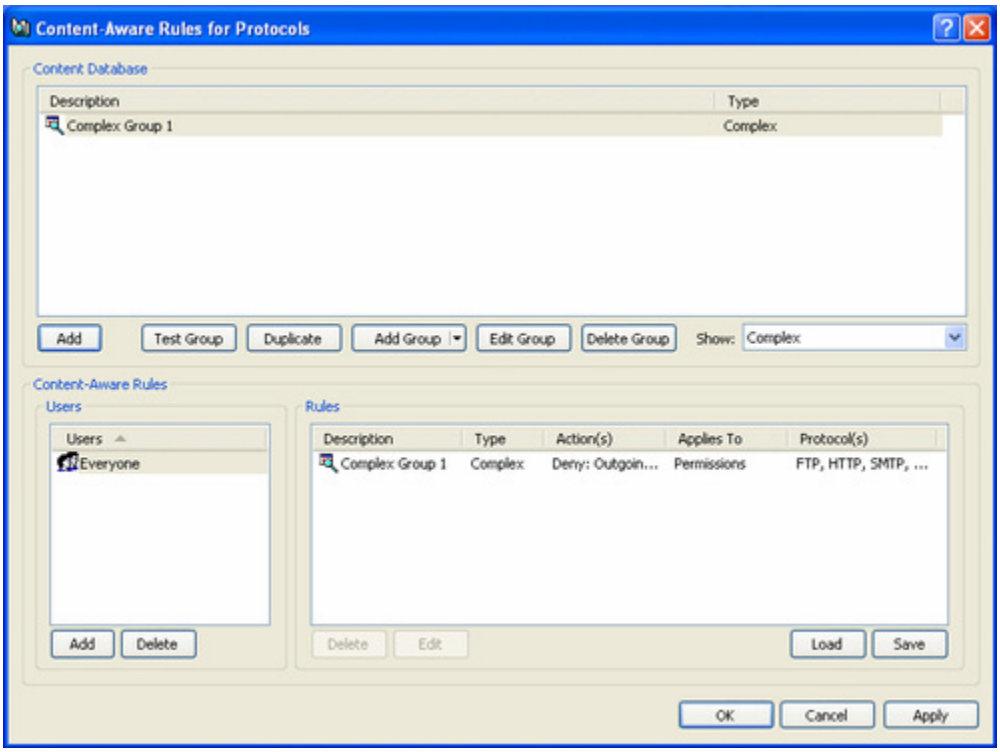


10. Dans la boîte de dialogue **Content-Aware Rules for Devices**, cliquez sur **OK** ou sur **Apply** pour appliquer la règle.
11. Dans l'arborescence de console, développez **Protocols**, cliquez droit sur **Content-Aware Rules**, puis cliquez sur **Manage**.

12. Dans la boîte de dialogue **Content-Aware Rules for Protocols**, procédez comme suit:
    a) Dans **Users**, cliquez sur **Add**. Dans le champ **Enter the object names to select** de la boîte de dialogue **Select Users or Groups**, saisissez **Everyone** puis cliquez sur **OK**.
    b) Dans **Users**, sélectionnez **Everyone**. Dans **Content Database**, sélectionnez le groupe de contenus **Complex Group 1**, puis cliquez sur **Add**.
13. Dans la boîte de dialogue **Add Rule**, procédez comme suit:
    a) Dans **Applies to**, cochez la case **Permissions**.
    b) Dans **Protocol(s)**, cochez les cases **FTP**, **HTTP**, **SMTP** et **Web Mail**.
    c) Dans **Action(s)**, cochez la case **Deny** située en regard des champs **Generic: Outgoing Files** et **SSL: Outgoing Files**.



    d) Cliquez sur **OK**.



14. Dans la boîte de dialogue **Content-Aware Rules for Protocols**, cliquez sur **OK** ou sur **Apply** pour appliquer la règle.